

kaspersky

Kaspersky Security Center 15 Linux

© 2024 AO Kaspersky Lab

Contenido

[Ayuda de Kaspersky Security Center Linux](#)

[Novedades](#)

[Acerca de Kaspersky Security Center Linux](#)

[Requisitos de hardware y software](#)

[Requisitos del Servidor de administración](#)

[Requisitos de Web Console](#)

[Requisitos del Agente de red](#)

[Aplicaciones y soluciones de Kaspersky compatibles](#)

[Sistemas operativos y plataformas incompatibles](#)

[Sistemas operativos y plataformas incompatibles. Servidor de administración](#)

[Sistemas operativos y plataformas incompatibles. Servidor de Kaspersky Security Center Web Console](#)

[Sistemas operativos y plataformas incompatibles. Agente de red](#)

[Kit de distribución](#)

[Acerca de la compatibilidad del Servidor de administración y Kaspersky Security Center Web Console](#)

[Comparación de Kaspersky Security Center: basado en Windows frente a basado en Linux](#)

[Acerca de Kaspersky Security Center Cloud Console](#)

[Arquitectura y conceptos básicos](#)

[Arquitectura](#)

[Diagrama de despliegue del Servidor de administración de Kaspersky Security Center Linux y Kaspersky Security Center Web Console](#)

[Puertos utilizados por Kaspersky Security Center Linux](#)

[Puertos usados por Kaspersky Security Center Web Console](#)

[Conceptos básicos](#)

[Servidor de administración](#)

[Jerarquía de Servidores de administración](#)

[Servidor de administración virtual](#)

[Servidor web](#)

[Agente de red](#)

[Grupos de administración](#)

[Dispositivo administrado](#)

[Dispositivo no asignado](#)

[Estación de trabajo del administrador](#)

[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](#)

[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, firewall en uso](#)

[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 Linux y las aplicaciones de seguridad: más información](#)

[Convenciones utilizadas en esquemas de interacción](#)

[Servidor de administración y DBMS](#)

[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](#)

[Primeros pasos](#)

[Instalación](#)

[Configurar el servidor MariaDB x64 para trabajar con Kaspersky Security Center Linux](#)

[Configurar el servidor PostgreSQL o Postgres Pro para trabajar con Kaspersky Security Center Linux](#)

[Escenario: autenticación del servidor PostgreSQL](#)

[Escenario: autenticación del servidor MySQL](#)

[Instalación de Kaspersky Security Center Linux](#)

[Instalación de Kaspersky Security Center Linux en modo silencioso](#)

[Instalación de Kaspersky Security Center Linux en Astra Linux en el modo de entorno de software cerrado](#)

[Instalación de Kaspersky Security Center Web Console](#)

[Parámetros de instalación de Kaspersky Security Center Web Console](#)

[Instalación de Kaspersky Security Center Web Console en Astra Linux en el modo de entorno de software cerrado](#)

[Instalación de Kaspersky Security Center Web Console conectado al Servidor de administración instalado en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux](#)

[Despliegue del clúster de conmutación por error de Kaspersky Security Center Linux](#)

[Escenario: Despliegue del clúster de conmutación por error de Kaspersky Security Center Linux](#)

[Sobre el clúster de conmutación por error de Kaspersky Security Center Linux](#)

[Preparación de un servidor de archivos para un clúster de conmutación por error de Kaspersky Security Center Linux](#)

[Preparación de nodos para un clúster de conmutación por error de Kaspersky Security Center Linux](#)

[Instalación de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux](#)

[Iniciar y detener nodos del clúster manualmente](#)

[Cuentas para trabajar con el DBMS](#)

[Configuración de la cuenta de DBMS para trabajar con MySQL y MariaDB](#)

[Configuración de la cuenta para trabajar con PostgreSQL y Postgres Pro](#)

[Certificados para trabajar con Kaspersky Security Center Linux](#)

[Acerca de los certificados de Kaspersky Security Center](#)

[Requisitos para los certificados personalizados que se utilizan en Kaspersky Security Center Linux](#)

[Reemisión del certificado de Kaspersky Security Center Web Console](#)

[Reemplazo del certificado de Kaspersky Security Center Web Console](#)

[Conversión de un certificado PFX al formato PEM](#)

[Escenario: 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](#)

[Definición de una carpeta compartida](#)

[Iniciar y cerrar sesión en Kaspersky Security Center Web Console](#)

[Cambiar el idioma de la interfaz de Kaspersky Security Center Web Console](#)

[Configuración del servidor MySQL x64 para trabajar con Kaspersky Security Center Linux](#)

[Asistente de inicio rápido](#)

- [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. Descarga de paquetes de distribución y creación de paquetes de instalación](#)
- [Paso 7. Configurar Kaspersky Security Network](#)
- [Paso 8. Selección del método de activación de la aplicación](#)
- [Paso 9. Creación de una configuración básica de protección de la red](#)
- [Paso 10. Configuración de notificaciones por correo electrónico](#)
- [Paso 11. Cerrar el asistente de inicio rápido](#)

[Asistente de despliegue de la protección](#)

[Iniciar Asistente de despliegue de la protección](#)

[Paso 1. Seleccionar el paquete de instalación](#)

[Paso 2. Selección de un método para la distribución del archivo de clave o código de activación](#)

[Paso 3. Seleccionar la versión del Agente de red](#)

[Paso 4. Seleccionar los dispositivos](#)

[Paso 5. Configurar la tarea de instalación remota](#)

[Paso 6. Eliminar aplicaciones incompatibles antes de la instalación](#)

[Paso 7. Mover los dispositivos a Dispositivos administrados](#)

[Paso 8. Seleccionar cuentas con acceso a los dispositivos](#)

[Paso 9. Iniciar la instalación](#)

[Actualización de Kaspersky Security Center Linux](#)

[Actualización de Kaspersky Security Center Linux mediante el archivo de instalación](#)

[Actualizar Kaspersky Security Center Linux mediante copia de seguridad](#)

[Actualización de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux](#)

[Actualización de Kaspersky Security Center Web Console](#)

[Instalar Kaspersky Security Center Web Console en Astra Linux en el modo de entorno de software cerrado](#)

[Migración a Kaspersky Security Center Linux](#)

[Exportación de objetos de grupo desde Kaspersky Security Center Windows](#)

[Importación del archivo de exportación en Kaspersky Security Center Linux](#)

[Cambio de dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux](#)

[Configuración del Servidor de administración](#)

[Configuración de la conexión de Kaspersky Security Center Web Console al Servidor de administración](#)

[Configurar una lista de direcciones IP permitidas para iniciar sesión en Kaspersky Security Center Linux](#)

[Configuración de las opciones de acceso a Internet para el Servidor de administración](#)

[Jerarquía de Servidores de administración](#)

[Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario](#)

[Ver la lista de servidores de administración secundarios](#)

[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](#)

[Visualización del registro de conexiones al Servidor de administración](#)

[Configuración del número máximo de eventos en el repositorio de eventos](#)

[Mover el Servidor de administración a otro dispositivo](#)

[Cambio de las credenciales de DBMS](#)

[Copia de seguridad y restauración de los datos del Servidor de administración](#)

[Crear una tarea de creación de copias de seguridad de los datos del Servidor de administración:](#)

[Uso de la utilidad kbackup para realizar copias de seguridad y recuperar datos](#)

[Mantenimiento del Servidor de administración](#)

[Eliminar una jerarquía de servidores de administración](#)

[Acceso a los servidores de DNS públicos](#)

[Configuración de la interfaz](#)

[Cifrar la comunicación con TLS](#)

[Descubrimiento de dispositivos conectados a la red](#)

[Escenario: Descubrir dispositivos conectados a la red](#)

[Sondeo de intervalos IP](#)

[Agregar y modificar un intervalo IP](#)

[Sondeo Zeroconf](#)

[Sondeo del controlador de dominio](#)

[Configuración de un controlador de dominio Samba](#)

[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](#)

[Mover los dispositivos que forman parte de la VDI a un grupo de administración](#)

[Prácticas recomendadas para el despliegue](#)

[Guía de protección](#)

[Despliegue del Servidor de administración](#)

[Seguridad de conexión](#)

[Cuentas y autenticación](#)

[Gestión de la protección del Servidor de administración](#)

[Gestión de la protección de dispositivos cliente](#)

[Configuración de la protección para aplicaciones administradas](#)

[Mantenimiento del Servidor de administración](#)

[Transferencia de eventos a sistemas de terceros](#)

[Preparativos para el despliegue](#)

[Planificación del despliegue de Kaspersky Security Center Linux](#)

[Esquemas típicos para desplegar un sistema de protección](#)

[Acerca de la planificación del despliegue de Kaspersky Security Center Linux en la red de una organización](#)

[Selección de una estructura para la protección de una empresa](#)

[Configuraciones estándares de Kaspersky Security Center Linux](#)

[Configuración estándar: oficina única](#)

[Configuración estándar: algunas oficinas a gran escala dirigidas por sus propios administradores](#)

[Configuración estándar: varias oficinas remotas pequeñas](#)

[Selección de un DBMS](#)

[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](#)

[Cálculo de la cantidad de puntos de distribución y su configuración](#)

[Servidores de administración virtuales](#)

[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](#)

[Acerca de las tareas de instalación remota en Kaspersky Security Center Linux](#)

[Despliegue mediante la captura y copia de la imagen de un dispositivo](#)

[Modo de clonación de disco del Agente de red](#)

[Despliegue forzado con la tarea de instalación remota de Kaspersky Security Center Linux](#)

[Ejecución de paquetes independientes creados por Kaspersky Security Center Linux](#)

[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](#)

[Supervisión del despliegue](#)

[Configuración de instaladores](#)

[Información general](#)

[Instalación en modo silencioso \(con un archivo de respuesta\)](#)

[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 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](#)

[Instalación manual de la tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security](#)

[Administración de dispositivos cliente](#)

[Configuración de un dispositivo administrado](#)

[Creación de grupos de administración](#)

[Reglas de movimiento de dispositivos](#)

[Crear reglas de movimiento de dispositivos](#)

[Copiar reglas de movimiento de dispositivos](#)

[Condiciones para una reglas de movimiento de dispositivos](#)

[Agregar dispositivos a un grupo de administración en forma manual](#)

[Traslado manual de dispositivos o clústeres al grupo de administración](#)

[Acerca de los clústeres y las matrices de servidores](#)

[Propiedades de un clúster o matriz de servidores](#)

[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](#)

[Cálculo de la cantidad de puntos de distribución y su configuración](#)

[Asignar puntos de distribución automáticamente](#)

[Designación manual de puntos de distribución](#)

[Modificar la lista de puntos de distribución para un grupo de administración](#)

[Habilitación de un servidor push](#)

[Acerca de los estados de los dispositivos](#)

[Configurar cambios de estado para los dispositivos](#)

[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](#)

[Acerca de las 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](#)

[Protección y cifrado de datos](#)

[Ver la lista de unidades cifradas](#)

[Ver la lista de eventos de cifrado](#)

[Crear y visualizar informes sobre cifrado](#)

[Brindar acceso a una unidad cifrada en modo sin conexión](#)

[Cambiar los dispositivos cliente de Servidor de administración](#)

[Ver y configurar las acciones para dispositivos inactivos](#)

[Envío de mensajes a usuarios de dispositivos](#)

[Encendido, apagado y reinicio remoto de dispositivos cliente](#)

[Despliegue de las aplicaciones de Kaspersky](#)

[Escenario: despliegue de aplicaciones de Kaspersky](#)

[Añadir complementos para aplicaciones de Kaspersky](#)

[Descargar y crear paquetes de instalación para aplicaciones de Kaspersky](#)

[Crear paquetes de instalación a partir de un archivo](#)

[Creación de paquetes de instalación independientes](#)

[Modificación del límite de datos para paquetes de instalación personalizados](#)

[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](#)

[Ver la lista de paquetes de instalación independientes](#)

[Distribución de paquetes de instalación a servidores de administración secundarios](#)

[Preparación de un dispositivo Linux e instalación del Agente de red en un dispositivo Linux de forma remota](#)

[Instalar aplicaciones mediante la tarea de instalación remota](#)

[Instalación de una aplicación de forma remota](#)

[Instalar aplicaciones en los Servidores de administración secundarios](#)

[Definir ajustes para instalaciones remotas en dispositivos Unix](#)

[Reemplazo de aplicaciones de seguridad de terceros](#)

[Eliminación de aplicaciones o actualizaciones de software de forma remota](#)

[Preparación de un dispositivo que ejecuta SUSE Linux Enterprise Server 15 para la instalación del Agente de red](#)

[Preparar un dispositivo Windows para la instalación remota. Utilidad Riprep](#)

[Preparar un dispositivo Windows para la instalación remota en modo interactivo](#)

[Preparar un dispositivo Windows para la instalación remota en modo silencioso](#)

[Licencias](#)

[Acerca de las licencias de Kaspersky Security Center Linux](#)

[Acerca del Contrato de licencia de usuario final](#)

[Acerca de la licencia](#)

[Acerca del certificado de licencia](#)

[Acerca de la clave de licencia](#)

[Ver la Política de privacidad](#)

[Opciones de licencias de Kaspersky Security Center](#)

[Acerca del archivo de clave](#)

[Sobre la provisión de datos](#)

[Acerca de la suscripción](#)

[Activación de Kaspersky Security Center Linux](#)

[Licencias de aplicaciones de Kaspersky administradas](#)

[Licencias de aplicaciones administradas](#)

[Agregar una clave de licencia al repositorio 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](#)

[Eventos sobre límites de licencia superados](#)

[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.](#)

[Configuración de las aplicaciones de Kaspersky.](#)

[Escenario: 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](#)

[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](#)

[Ajustes generales de una directiva](#)

[Modificar 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](#)

[Sincronización forzada](#)

[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](#)

[Copiar un perfil de directiva](#)

[Crear una regla de activación para un perfil de directiva](#)

[Eliminar un perfil de directiva](#)

[Ajustes de la directiva del Agente de red](#)

[Uso del Agente de red para Windows, Linux y macOS: comparación](#)

[Comparación de la configuración del Agente de red por sistemas operativos](#)

[Configuración manual de la directiva de Kaspersky Endpoint Security](#)

[Configurar Kaspersky Security Network](#)

[Comprobar la lista de las redes protegidas por Firewall](#)

[Desactivación del análisis de los dispositivos de red](#)

[Excluir detalles de software de la memoria del Servidor de administración](#)

[Configuración del acceso a la interfaz de Kaspersky Endpoint Security para Windows en 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](#)

[Kaspersky Security Network \(KSN\)](#)

[Acerca de KSN](#)

[Configurar el acceso a KSN](#)

[Habilitar y deshabilitar 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](#)

[Administración de 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](#)

[Inicio del asistente para cambiar contraseñas de tareas](#)

[Paso 1. Especificar credenciales](#)

[Paso 2. Seleccionar una acción para realizar](#)

[Paso 3. Ver los resultados](#)

[Ver resultados de la ejecución de tareas almacenados en el Servidor de administración](#)

[Etiquetas de aplicación](#)

[Acerca de las 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](#)

[Concesión de acceso sin conexión al dispositivo externo bloqueado por Control de dispositivos](#)

[Uso de la utilidad klscflag para abrir el puerto 13291](#)

[Registro de la aplicación Kaspersky Industrial CyberSecurity for Networks en Kaspersky Security Center Web Console](#)

[Administración de usuarios y roles de usuario](#)

[Acerca de las cuentas de usuario](#)

[Acerca de los roles 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](#)

[Asignación de derechos de acceso a usuarios y grupos](#)

[Agregar una cuenta de un usuario interno](#)

[Creación de un grupo de seguridad](#)

[Editar una cuenta de un usuario interno](#)

[Edición de un grupo de seguridad](#)

[Asignación de un rol a un usuario o grupo de seguridad](#)

[Adición de cuentas de usuario a un grupo de seguridad interno](#)

[Designación de un usuario como propietario de un dispositivo](#)

[Habilitación de la protección de una cuenta desde la modificación no autorizada](#)

[Verificación en dos pasos](#)

[Escenario: configurar la verificación en dos pasos para todos los usuarios](#)

[Acerca de la verificación en dos pasos de una cuenta](#)

[Habilitación de la verificación en dos pasos para su cuenta](#)

[Activación de la verificación en dos pasos para todos los usuarios](#)

[Deshabilitar la verificación en dos pasos para una cuenta de usuario](#)

[Deshabilitar la verificación en dos pasos para todos los usuarios](#)

[Excluir cuentas de la verificación en dos pasos](#)

[Configuración de la verificación en dos pasos para su cuenta](#)

[Prohibir a los nuevos usuarios configurar la verificación en dos pasos por sí mismos](#)

[Generar una nueva clave secreta](#)

[Editar el nombre del emisor de un código de seguridad](#)

[Cambiar el número de intentos de entrada de contraseña permitidos](#)

[Eliminar un usuario o un grupo de seguridad](#)

[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](#)

[Actualización de las bases de datos y las aplicaciones de Kaspersky](#)

[Escenario: 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](#)

[Crear una tarea para descargar las actualizaciones en los repositorios de los puntos de distribución](#)

[Adición de fuentes de actualizaciones para la tarea Descargar actualizaciones al repositorio del Servidor de administración](#)

[Acerca de la utilización de archivos diff para actualizar las bases de datos y los módulos de software de Kaspersky](#)

[Activación de la función de descarga de archivos diff: escenario](#)

[Descarga de actualizaciones por puntos de distribución](#)

[Actualizar las bases de datos y los módulos de software de Kaspersky en dispositivos sin conexión](#)

[Copia de seguridad y restauración de complementos web](#)

[Supervisión, generación de informes y auditoría](#)

[Escenario: 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](#)

[Generación y visualización de un informe](#)

[Crear una tarea de entrega de informes](#)

[Eliminación de plantillas de informes](#)

[Eventos y selecciones de eventos](#)

[Acerca de los eventos en Kaspersky Security Center Linux](#)

[Eventos de los componentes de Kaspersky Security Center Linux](#)

[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 Advertencia](#)

[Eventos del Agente de red: nivel Información](#)

[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](#)

[Bloquear eventos frecuentes](#)

[Acerca del bloqueo de eventos frecuentes](#)

[Administrar el bloqueo de eventos frecuentes](#)

[Eliminar el bloqueo de eventos frecuentes](#)

[Almacenamiento y procesamiento de eventos en el Servidor de administración](#)

[Notificaciones y estados de los dispositivos](#)

[Uso de notificaciones](#)

[Visualización de notificaciones en pantalla](#)

[Acerca de los estados de los dispositivos](#)

[Configurar cambios de estado para los dispositivos](#)

[Configurar el envío de notificaciones](#)

[Notificaciones de prueba](#)

[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](#)

[Exportación de eventos a sistemas SIEM](#)

[Escenario: Configurar la exportación de eventos a un sistema SIEM](#)

[Antes de comenzar](#)

[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 Syslog](#)

[Configuración de Kaspersky Security Center Linux para la exportación de eventos a un sistema SIEM](#)

[Exportación de eventos directamente desde la base de datos](#)

[Creación de una consulta de SQL usando la utilidad klsq|2](#)

[Ejemplo de una consulta de SQL usando la utilidad klsq|2](#)

[La visualización del nombre de la base de datos de Kaspersky Security Center Linux](#)

[Ver los resultados de la exportación](#)

[Administración de revisiones de objetos](#)

[Acerca de las revisiones de objetos](#)

[Devolver un objeto a una revisión anterior](#)

[Eliminación de objetos](#)

[Descarga y eliminación de archivos de Cuarentena y Copia de seguridad](#)

[Descarga de archivos de Cuarentena y Copia de seguridad](#)

[Acerca de la eliminación de objetos de los repositorios de Cuarentena, Copia de seguridad o Amenazas activas](#)

[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 información del sistema desde un dispositivo cliente](#)

[Descargar registros de eventos](#)

[Iniciar, detener o reiniciar la aplicación](#)

[Ejecutar los diagnósticos remotos del Agente de red de Kaspersky Security Center Linux 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](#)

[Administración de aplicaciones de terceros en dispositivos cliente](#)

[Escenario: Administración de aplicaciones](#)

[Acerca de Control de aplicaciones](#)

[Obtener y ver una lista de aplicaciones instaladas en los dispositivos cliente](#)

[Obtención y visualización de una lista de archivos ejecutables almacenados en los dispositivos cliente](#)

[Creación de una categoría de aplicaciones con contenido agregado manualmente](#)

[Crear una categoría de aplicaciones con archivos ejecutables de dispositivos específicos](#)

[Crear una categoría de aplicación que incluya archivos ejecutables de la carpeta seleccionada](#)

[Visualización de la lista de categorías de aplicaciones](#)

[Configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows](#)

[Agregar archivos ejecutables vinculados a eventos a una categoría de aplicaciones](#)

[Guía de referencia de API](#)

[Guía de dimensionamiento](#)

[Acerca de esta Guía](#)

[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](#)

[Evaluación de espacio en el disco](#)

[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 puertos 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 de la base de datos](#)

[Tareas de grupo para actualizar Kaspersky Endpoint Security](#)

[Tarea del inventario del software](#)

[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](#)

[Comunicarse con soporte técnico](#)

[Cómo obtener soporte técnico](#)

[Consultas mediante Kaspersky CompanyAccount al servicio de soporte técnico](#)

[Fuentes de información acerca de la aplicación](#)

[Problemas conocidos](#)

[Glosario](#)

[Actualización](#)

[Actualización disponible](#)

[Administración centralizada de aplicaciones](#)

[Administración directa de aplicaciones](#)

[Administrador de Kaspersky Security Center Linux](#)

[Administrador del cliente](#)

[Administrador del proveedor de servicios](#)

[Agente de autenticación](#)

[Agente de red](#)

[Aplicación incompatible](#)

[Archivo de clave](#)

[Bases de datos antivirus](#)

[Carpeta Copia de seguridad](#)

[Certificado compartido](#)

[Certificado del Servidor de administración](#)

[Clave activa](#)

[Clave de suscripción adicional](#)

[Cliente del Servidor de administración \(dispositivo cliente\)](#)

[Configuración de la tarea](#)

[Configuración de programa](#)

[Consola de administración](#)

[Copia de seguridad de los datos del Servidor de administración](#)

[Derechos de administrador](#)

[Directiva](#)

[Dispositivos administrados](#)

[Dominio de difusión](#)

[Estación de trabajo del administrador](#)

[Estado de protección](#)

[Estado de protección de la red](#)

[Gravedad de un evento](#)

[Grupo de administración](#)

[Grupo de aplicaciones con licencia](#)

[Grupo de roles](#)

[HTTPS](#)

[Instalación local](#)

[Instalación manual](#)

[Instalación remota](#)

[JavaScript](#)

[Kaspersky Private Security Network \(KPSN\)](#)

[Kaspersky Security Center System Health Validator \(SHV\)](#)

[Operador de Kaspersky Security Center](#)

[Paquete de instalación](#)

[Perfil](#)

[Perfil de aprovisionamiento](#)

[Perfil de configuración](#)

[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 web de Kaspersky Security Center Linux](#)
[Servidores de actualizaciones de Kaspersky](#)
[SSL](#)
[Tarea](#)
[Tarea de grupo](#)
[Tarea local](#)
[Tarea para dispositivos específicos](#)
[Tienda de aplicaciones](#)
[Usuarios internos](#)
[Zona desmilitarizada \(DMZ\)](#)
[Información sobre el código de terceros](#)
[Avisos de marcas registradas](#)

Ayuda de Kaspersky Security Center Linux

	<p><u>Novedades</u> Descubra las novedades de la última versión de la aplicación.</p>		<p><u>Aplicaciones de Kaspersky. Licencias y activación</u> Active las aplicaciones de Kaspersky en unos pocos pasos.</p>
	<p><u>Reemplazo de aplicaciones de seguridad de terceros</u> Aprende métodos para desinstalar aplicaciones incompatibles.</p>		<p><u>Guía de dimensionamiento (Ayuda en línea únicamente)</u> 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 Linux que necesita.</p>
	<p><u>Requisitos de hardware y software</u> Compruebe qué sistemas operativos y versiones de aplicaciones son compatibles.</p>		<p><u>Configurar la protección de la red</u> Administrar la seguridad de la organización.</p>
	<p><u>Instalación</u> Instale el Servidor de administración y Kaspersky Security Center Web Console.</p>		<p><u>Aplicaciones de Kaspersky. Actualización de bases de datos y módulos de software</u> Mantenga la fiabilidad del sistema de protección.</p>
	<p><u>Descubrimiento de dispositivos conectados a la red</u> Descubra los dispositivos nuevos y existentes en la red de su organización.</p>		<p><u>Supervisión e informes</u> Ver su infraestructura, estados de protección y estadísticas.</p>
	<p><u>Aplicaciones de Kaspersky. Despliegue centralizado</u> 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.</p>		<p><u>Ajuste de puntos de distribución y/o puertas de enlace de conexión</u> Configure sus puntos de distribución.</p>
	<p><u>Exportación de eventos a sistemas SIEM</u> Configure la exportación de eventos a los sistemas SIEM para su análisis.</p>		

Novedades

Kaspersky Security Center 15 Linux

Kaspersky Security Center 15 Linux tiene varias mejoras y funciones nuevas:

- El [sondeo del controlador de dominio](#) le permite sondear un controlador de dominio Microsoft Active Directory y un controlador de dominio Samba. Puede utilizar el Servidor de administración o un punto de distribución para sondear Microsoft Active Directory. Puede sondear un controlador de dominio Samba solo a través de un punto de distribución basado en Linux. 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.
- Kaspersky Security Center Linux ahora admite el trabajo con los siguientes [DBMS](#):
 - PostgreSQL 15.x
 - Postgres Pro 15.x
- Si utiliza PostgreSQL o Postgres Pro como DBMS, Kaspersky Security Center Linux admite [hasta 50 000 dispositivos administrados](#).
- Migración de Kaspersky Security Center Windows a Kaspersky Security Center Linux. Puede ejecutar un asistente para migrar los objetos de Kaspersky Security Center, incluidas las tareas, las directivas y la estructura del grupo de administración. Después de eso, puede mover los dispositivos administrados importados para que estén bajo la administración de Kaspersky Security Center Linux.
- Kaspersky Security Center Linux ahora admite el trabajo con las siguientes aplicaciones de [Kaspersky](#):
 - Kaspersky Security for Virtualization Light Agent
 - Kaspersky Embedded Systems Security para Windows
 - Kaspersky Embedded Systems Security para Linux
 - Kaspersky Industrial CyberSecurity for Nodes
 - Kaspersky Industrial CyberSecurity for Networks
 - Kaspersky Endpoint Security for Mac
 - Kaspersky Endpoint Agent
 - Kaspersky Security for Virtualization Light Agent
- [Diagnóstico remoto](#) de dispositivos administrados basados en Windows y Linux.
- Componente Control de aplicaciones mejorado. Ahora puede crear una categoría de aplicación basada en la lista de archivos ejecutables [de una carpeta seleccionada](#) o [en función de una categoría de aplicación de Kaspersky](#). Luego puede especificar si desea permitir o bloquear las aplicaciones de la categoría creada en su organización.
- Exportación e importación de selecciones de eventos. Puede [exportar una selección de eventos definida por el usuario](#) y su configuración a un archivo KLO, y luego [importar la selección de eventos guardada](#) a Kaspersky Security Center Windows o Kaspersky Security Center Linux.

- En el [Informe de amenazas](#), ahora puede abrir una cadena de desarrollo de amenazas haciendo clic en el enlace **Ver alerta**.
- Kaspersky Security Center Linux ahora admite la tecnología de clústeres. Si un grupo de administración contiene [clústeres o matrices de servidores](#), la página **Dispositivos administrados** muestra dos pestañas: una para dispositivos individuales y otra para clústeres y matrices 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 **Matrices de servidores y clústeres**. Los nodos de los clústeres se enumeran en la pestaña **Dispositivos**, junto con otros dispositivos administrados.
- [El soporte para algunas plataformas por parte de Kaspersky Security Center Linux](#) ha finalizado porque sus proveedores ya no les ofrecen soporte.

Kaspersky Security Center 14.2 Linux

Kaspersky Security Center 14.2 Linux tiene varias mejoras y funciones nuevas:

- Ahora, en una [jerarquía de servidores de administración](#), un Servidor de administración basado en Linux puede actuar como Servidor principal y puede administrar Servidores basados en Linux o Windows que actúan como servidor secundario.
- Ahora, Kaspersky Security Center Linux es compatible con [Kaspersky Security Network \(KSN\)](#), [Servicio de proxy de KSN](#) y Kaspersky Private Security Network (KPSN).
- [Kaspersky Security Center Linux ahora es compatible con Kaspersky Endpoint Security para Windows](#) como una aplicación administrada.

La instalación remota del Agente de red para Windows en dispositivos cliente solo es posible mediante el uso de herramientas del sistema operativo a través de puntos de distribución basados en Windows.

- [Ahora, los datos que hay en dispositivos administrados basados en Windows se pueden cifrar](#) para reducir el riesgo de fugas no intencionadas de datos confidenciales y corporativos en caso de robo o pérdida de su equipo portátil o disco duro. Esta función se implementa a través de Kaspersky Endpoint Security para Windows.
- Kaspersky Security Center Linux le permite descargar y actualizar ambos [paquetes de distribución de aplicaciones Kaspersky](#) y complementos web de administración directamente en la interfaz de usuario de Kaspersky Security Center Linux.
- De manera predeterminada, la información sobre las aplicaciones instaladas en los dispositivos administrados basados en Linux y Windows se envía al Servidor de administración.
- El acceso a los servidores de Kaspersky ahora se verifica automáticamente. Si no es posible acceder a los servidores usando el DNS del sistema, la aplicación utiliza el DNS público.
- Los datos confidenciales que se transfieren entre el Servidor de administración principal, los Servidores de administración secundarios y los Agentes de red ahora están protegidos con el algoritmo de cifrado AES.
- Los [derechos de usuario en un Servidor de administración virtual](#) están disponibles para su configuración en cualquier momento, independientemente del Servidor de administración principal. Además, puede asignar a los usuarios del servidor principal los derechos para administrar un servidor virtual.
- Kaspersky Security Center Linux ahora admite el trabajo con los siguientes [DBMS](#):
 - PostgreSQL 13.x
 - PostgreSQL 14.x

- Postgres Pro 13.x (todas las ediciones)
- Postgres Pro 14.x (todas las ediciones)
- Puede usar Kaspersky Security Center Web Console para [exportar directivas](#) y [tareas](#) a un archivo, y luego [importar las directivas](#) y [tareas](#) a Kaspersky Security Center Windows o Kaspersky Security Center Linux.
- La opción **No use servidor proxy** se ha eliminado de las siguientes tareas:
 - *Descargar actualizaciones en el repositorio del Servidor de administración*
 - *Descargar actualizaciones en los repositorios de puntos de distribución*

Kaspersky Security Center 14 Linux

Kaspersky Security Center Linux tiene varias mejoras y funciones nuevas:

- Además de con la tarea [Descargar actualizaciones en el repositorio del Servidor de administración](#), las bases de datos antivirus para las aplicaciones de seguridad de Kaspersky ahora se pueden descargar a través de la tarea [Descargar actualizaciones en los repositorios de puntos de distribución](#).
- Las bases de datos antivirus y los módulos de aplicaciones en los dispositivos administrados se pueden propagar y actualizar a través del Servidor de administración o los puntos de distribución. Puede [elegir un esquema de actualización](#) óptimo para su organización, para reducir la carga en el Servidor de administración y optimizar el tráfico de datos en la red corporativa.
- Kaspersky Security Center Linux descarga de los servidores de actualización de Kaspersky solo aquellas actualizaciones solicitadas por las aplicaciones de seguridad de Kaspersky. Esto reduce el volumen de los datos descargados.
- Ahora puede utilizar la [característica diff de archivos](#) para descargar bases de datos antivirus y módulos de software. 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.
- Se ha añadido la tarea [Verificación de actualizaciones](#). Al utilizar esta tarea, puede verificar automáticamente la operatividad y los errores de las actualizaciones descargadas antes de instalarlas en los dispositivos administrados.
- [Kaspersky Security Center Linux ahora es compatible con Kaspersky Industrial CyberSecurity for Linux Nodes 1.3](#) como una aplicación administrada.

Acerca de Kaspersky Security Center Linux

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

Kaspersky Security Center Linux (también conocido como Kaspersky Security Center) está diseñado para implementar y administrar la protección de dispositivos cliente mediante el Servidor de administración basado en Linux.

Kaspersky Security Center Linux le permite instalar aplicaciones de seguridad de Kaspersky en dispositivos de una red corporativa, ejecutar tareas de análisis y actualización de forma remota y administrar las políticas de seguridad de las aplicaciones administradas. Como administrador, puede usar un panel detallado que proporciona una instantánea de los estados de los dispositivos corporativos, informes detallados y configuraciones granulares en las políticas de protección.

En comparación con la versión de Kaspersky Security Center que tiene un servidor de administración basado en Windows®, Kaspersky Security Center Linux tiene un [conjunto de características diferente](#).

Kaspersky Security Center Linux es una aplicación pensada para administradores de redes corporativas y empleados responsables de la protección de dispositivos en 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.
- Realice la instalación remota de aplicaciones de Kaspersky y otros proveedores de software.
- 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.
- Administre el cifrado de la información almacenada en los discos duros de los dispositivos basados en Windows y las unidades extraíbles.
- Administre el acceso de los usuarios a los datos cifrados en dispositivos basados en Windows.
- 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 Linux a través de Kaspersky (por ejemplo, en <https://kaspersky.es>) o a través de empresas asociadas.

Si compra Kaspersky Security Center Linux 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.

Requisitos de hardware y software

- [Requisitos del Servidor de administración](#)
- [Requisitos de Web Console](#)
- [Requisitos del Agente de red](#)

Requisitos del Servidor de administración

Requisitos de hardware mínimos:

- CPU con frecuencia de operación de 1 GHz o superior. Para sistemas operativos de 64 bits, la frecuencia mínima admisible es de 1.4 GHz.
- RAM: 4 GB.
- Espacio disponible en disco: 10 GB (/ var / opt / kaspersky / klnagent_srv).

Se admiten los siguientes sistemas operativos:

- Debian GNU/Linux 10.x (Buster) (64 bits)
- Debian GNU/Linux 11.x (Bullseye) (64 bits)
- Debian GNU/Linux 12 (Bookworm) de 64 bits
- Ubuntu Server 18.04 LTS (Bionic Beaver) (64 bits)
- Ubuntu Server 20.04 LTS (Focal Fossa) (64 bits)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) (64 bits)
- CentOS 7.x (64 bits)
- CentOS Stream 9 de 64 bits
- Red Hat Enterprise Linux Server 7.x (64 bits)
- Red Hat Enterprise Linux Server 8.x (64 bits)
- Red Hat Enterprise Linux Server 9.x (64 bits)
- SUSE Linux Enterprise Server 12, todos los Service Pack (64 bits)
- SUSE Linux Enterprise Server 15, todos los Service Pack (64 bits)

- Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.6) (64 bits)
- Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.7) (64 bits)
- Astra Linux Common Edition (actualización operativa 2.12) (64 bits)
- ALT SP Server 10 de 64 bits
- ALT Server 10 (64 bits)
- ALT Server 9.2 (64 bits)
- ALT 8 SP Server (LKNV.11100-01) (64 bits)
- ALT 8 SP Server (LKNV.11100-02) (64 bits)
- ALT 8 SP Server (LKNV.11100-03) (64 bits)
- Oracle Linux 7 (64 bits)
- Oracle Linux 8 (64 bits)
- Oracle Linux 9 (64 bits)
- RED OS 7.3 Server (64 bits)
- RED OS 7.3 Certified Edition (64 bits)
- ROSA COBALT 7.9 (64 bits)

Le recomendamos que utilice el sistema de archivos EXT4 con su configuración predeterminada.

Se admiten las siguientes plataformas de virtualización:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 (64 bits)
- Microsoft Hyper-V Server 2012 R2 (64 bits)
- Microsoft Hyper-V Server 2016 (64 bits)
- 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 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- Máquina virtual basada en kernel (todos los sistemas operativos Linux compatibles con el Servidor de administración)

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

- MySQL 5.7 Community (32 bits o 64 bits)
- MySQL 8.0 de (32 bits o 64 bits)
- MariaDB 10.1 (compilación 10.1.30 en adelante) (32 bits o 64 bits)
- MariaDB 10.3 (compilación 10.3.22 y posteriores) (32 bits o 64 bits)
- MariaDB 10.4 (compilación 10.4.26 en adelante) (32 bits o 64 bits)
- MariaDB 10.5 (compilación 10.5.17 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 de 64 bits
- PostgreSQL 14.x de 64 bits
- PostgreSQL 15.x de 64 bits
- Postgres Pro 13.x de 64 bits (todas las ediciones)
- Postgres Pro 14.x de 64 bits (todas las ediciones)
- Postgres Pro 15.x de 64 bits (todas las ediciones)
- Platform V Pangolin 5.4.0 de 64 bits
- Jatoba 4 de 64 bits

Requisitos de Web Console

Servidor de Kaspersky Security Center Web Console

Requisitos de hardware mínimos:

- CPU: 4 núcleos, frecuencia de operación de 2,5 GHz.
- RAM: 8 GB.
- Espacio disponible en disco: 40 GB (/ var / opt / kaspersky).

Uno de los siguientes sistemas operativos (solo versiones de 64 bits):

- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 11.x (Bullseye)
- Debian GNU/Linux 12 (Bookworm)
- Ubuntu Server 18.04 LTS (Bionic Beaver)
- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- CentOS Stream 9
- Red Hat Enterprise Linux Server 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 9.x
- SUSE Linux Enterprise Server 12 (todos los Service Pack)
- SUSE Linux Enterprise Server 15 (todos los Service Pack)
- Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.6)
- Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.7)
- Astra Linux Common Edition (actualización operativa 2.12)
- ALT SP Server 10
- ALT Server 10
- ALT Server 9.2
- ALT 8 SP Server (LKNV.11100-01)
- ALT 8 SP Server (LKNV.11100-02)
- ALT 8 SP Server (LKNV.11100-03)
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9

- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- ROSA COBALT 7.9
- Máquina virtual basada en kernel (todos los sistemas operativos Linux compatibles con Kaspersky Security Center Web Console Server)

Dispositivos cliente

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

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 100.0.4896.88 y versiones posteriores (compilación oficial)
- Microsoft Edge 100 y versiones posteriores
- Safari 15 en macOS
- "Yandex" Browser 23.5.0.2271 y versiones posteriores
- Mozilla Firefox Extended Support Release 102.0 y versiones posteriores

Requisitos del Agente de red

Requisitos de hardware mínimos:

- CPU con frecuencia de operación de 1 GHz o superior. 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 basados en Linux: debe estar instalado el intérprete de lenguaje Perl versión 5.10 o superior.

Se admiten los siguientes sistemas operativos:

- Microsoft Windows Embedded POSReady 2009 con el Service Pack más reciente (32 bits)
- Microsoft Windows Embedded 7 Standard con Service Pack 1 (32 bits o 64 bits)
- Microsoft Windows Embedded 8.1 Industry Pro (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise 2015 LTSC (32 bits o 64 bits)

- Microsoft Windows 10 Enterprise 2016 LTSC (32 bits o 64 bits)
- Microsoft Windows 10 IoT Enterprise 2015 LTSC (32 bits o 64 bits)
- Microsoft Windows 10 IoT Enterprise 2016 LTSC (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise 2019 LTSC (32 bits o 64 bits)
- Microsoft Windows 10 IoT Enterprise versión 1703 (32 bits o 64 bits)
- Microsoft Windows 10 IoT Enterprise versión 1709 (32 bits o 64 bits)
- Microsoft Windows 10 IoT Enterprise version 1803 (32 bits o 64 bits)
- Microsoft Windows 10 IoT Enterprise version 1809 (32 bits o 64 bits)
- Microsoft Windows 10 20H2 IoT Enterprise (32 bits o 64 bits)
- Microsoft Windows 10 21H2 IoT Enterprise (32 bits o 64 bits)
- Microsoft Windows 10 IoT Enterprise (32 bits o 64 bits)
- Microsoft Windows 10 IoT Enterprise versión 1909 (32 bits o 64 bits)
- Microsoft Windows 10 IoT Enterprise LTSC 2021 (32 bits o 64 bits)
- Microsoft Windows 10 IoT Enterprise version 1607 (32 bits o 64 bits)
- Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) (32 bits o 64 bits)
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) (32 bits o 64 bits)
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) (32 bits o 64 bits)
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) (32 bits o 64 bits)
- Microsoft Windows 10 Home RS4 (actualización de abril de 2018, 17134) (32 bits o 64 bits)
- Microsoft Windows 10 Pro RS4 (actualización de abril de 2018, 17134) (32 bits o 64 bits)
- Microsoft Windows 10 Pro for Workstations RS4 (actualización de abril de 2018, 17134) (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise RS4 (actualización de abril de 2018, 17134) (32 bits o 64 bits)
- Microsoft Windows 10 Education RS4 (actualización de abril de 2018, 17134) (32 bits o 64 bits)
- Microsoft Windows 10 Home RS5 (octubre de 2018) (32 bits o 64 bits)
- Microsoft Windows 10 Pro RS5 (Octubre de 2018) (32 bits o 64 bits)
- Microsoft Windows 10 Pro for Workstations RS5 (Octubre de 2018) (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise RS5 (Octubre de 2018) (32 bits o 64 bits)

- Microsoft Windows 10 Education RS5 (Octubre de 2018) (32 bits o 64 bits)
- Microsoft Windows 10 Home 19H1 (32 bits o 64 bits)
- Microsoft Windows 10 Pro 19H1 (32 bits o 64 bits)
- Microsoft Windows 10 Pro for Workstations 19H1 (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise 19H1 (32 bits o 64 bits)
- Microsoft Windows 10 Education 19H1 (32 bits o 64 bits)
- Microsoft Windows 10 Home 19H2 (32 bits o 64 bits)
- Microsoft Windows 10 Pro 19H2 (32 bits o 64 bits)
- Microsoft Windows 10 Pro for Workstations 19H2 (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise 19H2 (32 bits o 64 bits)
- Microsoft Windows 10 Education 19H2 (32 bits o 64 bits)
- Microsoft Windows 10 Home 20H1 (actualización de mayo de 2020) (32 bits o 64 bits)
- Microsoft Windows 10 Pro 20H1 (actualización de mayo de 2020) (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise 20H1 (actualización de mayo de 2020) (32 bits o 64 bits)
- Microsoft Windows 10 Education 20H1 (actualización de mayo de 2020) (32 bits o 64 bits)
- Microsoft Windows 10 Home 20H2 (actualización de octubre de 2020) (32 bits o 64 bits)
- Microsoft Windows 10 Pro 20H2 (actualización de octubre de 2020) (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise 20H2 (actualización de octubre de 2020) (32 bits o 64 bits)
- Microsoft Windows 10 Education 20H2 (actualización de octubre de 2020) (32 bits o 64 bits)
- Microsoft Windows 10 Home 21H1 (actualización de mayo de 2021) (32 bits o 64 bits)
- Microsoft Windows 10 Pro 21H1 (actualización de mayo de 2021) (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise 21H1 (actualización de mayo de 2021) (32 bits o 64 bits)
- Microsoft Windows 10 Education 21H1 (actualización de mayo de 2021) (32 bits o 64 bits)
- Microsoft Windows 10 Home 21H2 (actualización de octubre de 2021) (32 bits o 64 bits)
- Microsoft Windows 10 Pro 21H2 (actualización de octubre de 2021) (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise 21H2 (actualización de octubre de 2021) (32 bits o 64 bits)
- Microsoft Windows 10 Education 21H2 (actualización de octubre de 2021) (32 bits o 64 bits)
- Microsoft Windows 10 Home 22H2 (actualización de octubre de 2023) (32 bits o 64 bits)

- Microsoft Windows 10 Pro 22H2 (actualización de octubre de 2023) (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise 22H2 (actualización de octubre de 2023) (32 bits o 64 bits)
- Microsoft Windows 10 Education 22H2 (actualización de octubre de 2023) (32 bits o 64 bits)
- Microsoft Windows 11 Home (64 bits)
- Microsoft Windows 11 Pro (64 bits)
- Microsoft Windows 11 Enterprise (64 bits)
- Microsoft Windows 11 Education (64 bits)
- Microsoft Windows 11 22H2
- Microsoft Windows 8.1 Pro (32 bits o 64 bits)
- Microsoft Windows 8.1 Enterprise (32 bits o 64 bits)
- Microsoft Windows 8 Pro (32 bits o 64 bits)
- Microsoft Windows 8 Enterprise (32 bits o 64 bits)
- Microsoft Windows 7 Professional con Service Pack 1 y versiones posteriores (32 bits o 64 bits)
- Microsoft Windows 7 Enterprise/Ultimate con Service Pack 1 y versiones posteriores (32 bits o 64 bits)
- Microsoft Windows 7 Professional con Service Pack 1 y versiones posteriores (32 bits o 64 bits)
- Microsoft Windows XP Professional con Service Pack 2 de 32 bits / 64 bits (compatible solo con la versión 10.5.1781 del Agente de red)
- Microsoft 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)
- Microsoft 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)
- Windows MultiPoint Server 2011 Standard/Premium (64 bits)
- Windows Server 2008 Foundation with Service Pack 2 (32 bits o 64 bits)
- Windows Server 2008 con Service Pack 2 (todas las ediciones) (32 bits o 64 bits)
- Windows Server 2008 R2 Datacenter con Service Pack 1 y versiones posteriores (64 bits)
- Windows Server 2008 R2 Enterprise con Service Pack 1 y versiones posteriores (64 bits)
- Windows Server 2008 R2 Foundation Service Pack 1 y versiones posteriores (64 bits)
- Windows Server 2008 R2 Core Mode con Service Pack 1 y versiones posteriores (64 bits)
- Windows Server 2008 R2 Standard con Service Pack 1 y versiones posteriores (64 bits)
- Windows Server 2008 R2 con Service Pack 1 (todas las ediciones) (64 bits)

- Windows Server 2012 Server Core (64 bits)
- Windows Server 2012 Datacenter (64 bits)
- Windows Server 2012 Essentials (64 bits)
- Windows Server 2012 Foundation (64 bits)
- Windows Server 2012 Standard (64 bits)
- Windows Server 2012 R2 Server Core (64 bits)
- Windows Server 2012 R2 Datacenter (64 bits)
- Windows Server 2012 R2 Essentials (64 bits)
- Windows Server 2012 R2 Foundation (64 bits)
- Windows Server 2012 R2 Standard (64 bits)
- Windows Server 2016 Datacenter (LTSB) (64 bits)
- Windows Server 2016 Standard (LTSB) (64 bits)
- Windows Server 2016 Server Core (opción de instalación) (LTSB) (64 bits)
- Windows Server 2019 Standard (64 bits)
- Windows Server 2019 Datacenter (64 bits)
- Windows Server 2019 Core (64 bits)
- Windows Server 2022 Standard (64 bits)
- Windows Server 2022 Datacenter (64 bits)
- Windows Server 2022 Core (64 bits)
- Debian GNU/Linux 10.x (Buster) de (32 bits o 64 bits)
- Debian GNU/Linux 11.x (Bullseye) (32 bits o 64 bits)
- Debian GNU/Linux 12 (Bookworm) de 32 bits o 64 bits
- Ubuntu Server 18.04 LTS (Bionic Beaver) (32 bits o 64 bits)
- Ubuntu Server 20.04 LTS (Focal Fossa) (32 bits o 64 bits)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) (64 bits)
- CentOS 7.x (64 bits)
- CentOS Stream 9 de 64 bits
- Red Hat Enterprise Linux Server 6.x (32 bits o 64 bits)

- Red Hat Enterprise Linux Server 7.x (64 bits)
- Red Hat Enterprise Linux Server 8.x (64 bits)
- Red Hat Enterprise Linux Server 9.x (64 bits)
- SUSE Linux Enterprise Server 12, todos los Service Pack (64 bits)
- SUSE Linux Enterprise Server 15, todos los Service Pack (64 bits)
- SUSE Linux Enterprise Desktop 15 con Service Pack 3 ARM (64 bits)
- openSUSE 15 (64 bits)
- EulerOS 2.0 SP8 (ARM)
- Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.6) (64 bits)
- Astra Linux Special Edition RUSB.10015-01 (actualización operativa 1.7) (64 bits)
- Astra Linux Common Edition (actualización operativa 2.12) (64 bits)
- Astra Linux Special Edition RUSB.10152-02 (actualización operativa 4.7) ARM (64 bits)
- ALT SP Server 10 de 64 bits
- ALT SP Workstation 10 de 64 bits
- ALT Server 10 (64 bits)
- ALT Server 9.2 (64 bits)
- ALT Workstation 9.2 (32 bits o 64 bits)
- ALT Workstation 10 (32 bits o 64 bits)
- ALT 8 SP Server (LKNV.11100-01) (64 bits)
- ALT 8 SP Server (LKNV.11100-02) (64 bits)
- ALT 8 SP Server (LKNV.11100-03) (64 bits)
- ALT 8 SP Workstation (LKNV.11100-01) (32 bits o 64 bits)
- ALT 8 SP Workstation (LKNV.11100-02) (32 bits o 64 bits)
- ALT 8 SP Workstation (LKNV.11100-03) (32 bits o 64 bits)
- Mageia 4 (32 bits)
- Oracle Linux 7 (64 bits)
- Oracle Linux 8 (64 bits)
- Oracle Linux 9 (64 bits)

- Linux Mint 20.x (64 bits)
 - AlterOS 7.5 y versiones posteriores (64 bits)
 - GosLinux IC6 (64 bits)
 - RED OS 7.3 (64 bits)
 - RED OS 7.3 Server (64 bits)
 - RED OS 7.3 Certified Edition (64 bits)
 - ROSA COBALT 7.9 (64 bits)
 - ROSA CHROME 12 (64 bits)
 - macOS Big Sur (11.x)
 - macOS Monterey (12.x)
 - macOS Ventura (13.x)
- 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
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 (64 bits)
- Microsoft Hyper-V Server 2012 R2 (64 bits)
- Microsoft Hyper-V Server 2016 (64 bits)
- 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 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x

- Máquina virtual basada en kernel (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 MultiPoint Server 2011, asegúrese de haber instalado la [actualización de seguridad para Windows 7 \(KB3063858\)](#).

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 requiera del Agente de red para Microsoft Windows XP [desde esta página](#).

Le recomendamos que instale la misma versión del Agente de red para Linux que en Kaspersky Security Center Linux.

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

Aplicaciones y soluciones de Kaspersky compatibles

Kaspersky Security Center Linux admite el despliegue centralizado y la administración de las siguientes aplicaciones y soluciones de Kaspersky:

- Kaspersky Endpoint Security para Windows 12.0 o posterior (admite servidores de archivos)
- Kaspersky Endpoint Security for Linux 11.2 o posterior (admite servidores de archivos)
- Kaspersky Endpoint Security for Linux Elbrus Edition 10 o versiones posteriores
- Kaspersky Endpoint Security for Linux ARM Edition 11.2 o posterior
- Kaspersky Endpoint Security for Mac 11.3 o versiones posteriores
- Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 o versiones posteriores
- Kaspersky Industrial CyberSecurity for Nodes 3.2 o versiones posteriores
- Kaspersky Industrial CyberSecurity for Networks 3.2 o versiones posteriores
- Kaspersky Endpoint Agent 3.15 o versiones posteriores

- Kaspersky Embedded Systems Security for Windows 3.2 o versiones posteriores
- Kaspersky Embedded Systems Security for Linux 3.3 o versiones posteriores
- Kaspersky Security for Virtualization Light Agent 5.2 o versiones posteriores

Consulte la [Página web del ciclo de vida del soporte del producto](#) para ver las versiones de las aplicaciones.

Problemas conocidos

Kaspersky Security Center Linux admite la administración de Kaspersky Endpoint Security para Windows con las siguientes limitaciones:

- El componente Control de anomalías adaptativo no es compatible. Kaspersky Security Center Linux no es compatible con las reglas de Control de anomalías adaptativo.
- Los componentes Kaspersky Sandbox no son compatibles.
- La característica Actualizaciones sin interrupciones no está disponible.

El inicio de sesión único (SSO) no es compatible con Kaspersky Industrial CyberSecurity for Networks.

Sistemas operativos y plataformas incompatibles

- [Sistemas operativos y plataformas incompatibles. Servidor de administración](#)
- [Sistemas operativos y plataformas incompatibles. Servidor de Kaspersky Security Center Web Console](#)
- [Sistemas operativos y plataformas incompatibles. Agente de red](#)

Sistemas operativos y plataformas incompatibles. Servidor de administración

El Servidor de administración no es compatible con los siguientes sistemas operativos:

- Debian GNU/Linux 7.x (hasta la versión 7.8) (32 bits o 64 bits)
- Debian GNU/Linux 8.x (Jessie) (32 bits o 64 bits)
- Debian GNU/Linux 9.x (Stretch) (32 bits o 64 bits)
- Ubuntu Server 14.04 LTS (Trusty Tahr) (32 bits o 64 bits)
- Ubuntu Server 16.04 LTS (Xenial Xerus) (32 bits o 64 bits)
- Ubuntu Server 18.04 LTS (Bionic Beaver) (32 bits)
- Ubuntu Server 20.04.04 LTS (Focal Fossa) (ARM de 64 bits)
- Ubuntu Server 20.04 LTS (Focal Fossa) (32 bits)

- Ubuntu Desktop 14.04 LTS (Trusty Tahr) (32 bits o 64 bits)
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) (32 bits o 64 bits)
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) (32 bits o 64 bits)
- Ubuntu Desktop 20.04 LTS (Focal Fossa) (32 bits o 64 bits)
- CentOS 6.x (hasta la versión 6.6) (64 bits)
- CentOS 7.x (ARM de 64 bits)
- CentOS 8.x (64 bits)
- Red Hat Enterprise Linux Server 6.x (32 bits o 64 bits)
- SUSE Linux Enterprise Desktop 12, todos los Service Pack (64 bits)
- SUSE Linux Enterprise Desktop 15, todos los Service Pack (64 bits)
- SUSE Linux Enterprise Desktop 15 con Service Pack 3 ARM (64 bits)
- openSUSE 15 (64 bits)
- EulerOS 2.0 SP8 (ARM)
- Pardus OS 19.1 (64 bits)
- Astra Linux Special Edition 1.5 (64 bits)
- Astra Linux Special Edition RUSB.10152-02 (actualización operativa 4.7) ARM (64 bits)
- ALT Workstation 9.2 (32 bits o 64 bits)
- ALT Workstation 10 (32 bits o 64 bits)
- ALT 8 SP Workstation (LKNV.11100-01) (32 bits o 64 bits)
- ALT 8 SP Workstation (LKNV.11100-02) (32 bits o 64 bits)
- ALT 8 SP Workstation (LKNV.11100-03) (32 bits o 64 bits)
- Mageia 4 (32 bits)
- Linux Mint 19.x (32 bits)
- Linux Mint 20.x (64 bits)
- AlterOS 7.5 y versiones posteriores (64 bits)
- RED OS 7.3 (64 bits)
- GosLinux IC6 (64 bits)
- ROSA Enterprise Linux Server 7.3 (64 bits)

- ROSA Enterprise Linux Desktop 7.3 (64 bits)
- ROSA COBALT Workstation 7.3 (64 bits)
- ROSA COBALT Server 7.3 (64 bits)
- ROSA CHROME 12 (64 bits)
- Lotos (versión del núcleo Linux: 4.19.50; entorno de escritorio: MATE) (64 bits)

Servidor de bases de datos:

- PostgreSQL Pangolin (64 bits)
- Microsoft SQL Server 2005 Express (32 bits)
- Microsoft SQL Server 2005 (todas las ediciones) (32 bits o 64 bits)
- Microsoft SQL Server 2008 Express (32 bits)
- Microsoft SQL Server 2008 (todas las ediciones) (32 bits o 64 bits)
- Microsoft SQL Server 2008 R2 (todas las ediciones) (64 bits)
- Windows SQL Server 2008 R2 con Service Pack 2 (todas las ediciones) (64 bits)
- Microsoft SQL Server 2012 (todas las ediciones) (64 bits)
- MySQL 5.0 (32 bits o 64 bits)
- MySQL Enterprise 5.0 (32 bits o 64 bits)
- MySQL Standard Edition 5.5 (32 bits o 64 bits)
- MySQL Enterprise Edition 5.5 (32 bits o 64 bits)
- MySQL Standard Edition 5.6 (32 bits o 64 bits)
- MySQL Enterprise Edition 5.6 (32 bits o 64 bits)
- MySQL Standard Edition 5.7 (32 bits o 64 bits)
- MySQL Enterprise Edition 5.7 (32 bits o 64 bits)
- MySQL 5.6 Community (32 bits o 64 bits)
- MariaDB Galera Cluster 10.4 (32 bits o 64 bits)

Las siguientes plataformas de virtualización son incompatibles:

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1

- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 (64 bits)
- Microsoft Hyper-V Server 2008 R2 (64 bits)
- Microsoft Hyper-V Server 2008 R2 con Service Pack 1 y posterior de 64 bits
- Microsoft Virtual PC 2007 (6.0.156.0) (32 bits o 64 bits)
- Citrix XenServer 5.6
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7
- Parallels Desktop 7
- Parallels Desktop 11
- Parallels Desktop 14
- Parallels Desktop 16
- Oracle VM VirtualBox 4.0.4-70112
- Oracle VM VirtualBox 5.x

Sistemas operativos y plataformas incompatibles. Servidor de Kaspersky Security Center Web Console

El Servidor de Kaspersky Security Center Web Console no es compatible con ninguno de los siguientes sistemas operativos:

- Debian GNU/Linux 7.x (hasta la versión 7.8) (32 bits o 64 bits)
- Debian GNU/Linux 8.x (Jessie) (32 bits o 64 bits)
- Debian GNU/Linux 9.x (Stretch) (32 bits o 64 bits)
- Ubuntu Server 14.04 LTS (Trusty Tahr) (32 bits o 64 bits)
- Ubuntu Server 16.04 LTS (Xenial Xerus) (32 bits o 64 bits)
- Ubuntu Server 20.04.04 LTS (Focal Fossa) (ARM de 64 bits)
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) (32 bits o 64 bits)
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) (32 bits o 64 bits)
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) (32 bits o 64 bits)
- Ubuntu Desktop 20.04 LTS (Focal Fossa) (32 bits o 64 bits)
- CentOS 6.x (hasta la versión 6.6) (64 bits)
- CentOS 7.x (ARM de 64 bits)
- CentOS 7.x (64 bits)
- CentOS 8.x (64 bits)
- Red Hat Enterprise Linux Server 6.x (32 bits o 64 bits)
- SUSE Linux Enterprise Desktop 12, todos los Service Pack (64 bits)
- SUSE Linux Enterprise Desktop 15, todos los Service Pack (64 bits)
- SUSE Linux Enterprise Desktop 15 con Service Pack 3 ARM (64 bits)
- openSUSE 15 (64 bits)
- EulerOS 2.0 SP8 (ARM)
- Pardus OS 19.1 (64 bits)
- Astra Linux Special Edition 1.5 (64 bits)
- Astra Linux Special Edition RUSB.10152-02 (actualización operativa 4.7) ARM (64 bits)
- ALT Workstation 9.2 (32 bits o 64 bits)
- ALT Workstation 10 (32 bits o 64 bits)
- ALT 8 SP Workstation (LKNV.11100-01) (32 bits o 64 bits)
- ALT 8 SP Workstation (LKNV.11100-02) (32 bits o 64 bits)

- ALT 8 SP Workstation (LKNV.11100-03) (32 bits o 64 bits)
- Mageia 4 (32 bits)
- Linux Mint 19.x (32 bits)
- Linux Mint 20.x (64 bits)
- AlterOS 7.5 y versiones posteriores (64 bits)
- RED OS 7.3 (64 bits)
- GosLinux IC6 (64 bits)
- ROSA Enterprise Linux Server 7.3 (64 bits)
- ROSA Enterprise Linux Desktop 7.3 (64 bits)
- ROSA COBALT Workstation 7.3 (64 bits)
- ROSA COBALT Server 7.3 (64 bits)
- ROSA CHROME 12 (64 bits)
- Lotos (versión del núcleo Linux: 4.19.50; entorno de escritorio: MATE) (64 bits)

Sistemas operativos y plataformas incompatibles. Agente de red

Los siguientes sistemas operativos son incompatibles:

- Microsoft Windows Embedded POSReady 7 (32 bits o 64 bits)
- Microsoft Windows Embedded 8 Standard (32 bits o 64 bits)
- Microsoft Windows Embedded 8 Industry Pro (32 bits o 64 bits)
- Microsoft Windows Embedded 8 Industry Enterprise (32 bits o 64 bits)
- Microsoft Windows Embedded 8.1 Industry Enterprise (32 bits o 64 bits)
- Microsoft Windows Embedded 8.1 Industry Update (32 bits o 64 bits)
- Microsoft Windows 10 Home (Threshold 1, 1507) (32 bits o 64 bits)
- Microsoft Windows 10 Pro (Threshold 1, 1507) (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise (Threshold 1, 1507) (32 bits o 64 bits)
- Microsoft Windows 10 Education (Threshold 1, 1507) (32 bits o 64 bits)
- Microsoft Windows 10 Mobile (Threshold 1, 1507) (32 bits)
- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) (32 bits)

- Microsoft Windows 10 Home Threshold 2 (actualización de noviembre de 2015, 1511) (32 bits o 64 bits)
- Microsoft Windows 10 Pro Threshold 2 (actualización de noviembre de 2015, 1511) (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise Threshold 2 (actualización de noviembre de 2015, 1511) (32 bits o 64 bits)
- Microsoft Windows 10 Education Threshold 2 (actualización de noviembre de 2015, 1511) (32 bits o 64 bits)
- Microsoft Windows 10 Mobile Threshold 2 (actualización de noviembre de 2015, 1511) (32 bits)
- Microsoft Windows 10 Mobile Enterprise Threshold 2 (actualización de noviembre de 2015, 1511) (32 bits)
- Microsoft Windows 10 Home RS1 (Actualización de aniversario, 1607) (32 bits o 64 bits)
- Microsoft Windows 10 Pro RS1 (Actualización de aniversario, 1607) (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise RS1 (Actualización de aniversario, 1607) (32 bits o 64 bits)
- Microsoft Windows 10 Education RS1 (Actualización de aniversario, 1607) (32 bits o 64 bits)
- Microsoft Windows 10 Mobile RS1 (Actualización de aniversario, 1607) (32 bits)
- Microsoft Windows 10 Mobile Enterprise RS1 (Actualización de aniversario, 1607) (32 bits)
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) (32 bits o 64 bits)
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) (32 bits o 64 bits)
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) (32 bits o 64 bits)
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) (32 bits o 64 bits)
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) (32 bits)
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) (32 bits)
- Microsoft Windows 10 Mobile RS3 (32 bits)
- Microsoft Windows 10 Mobile Enterprise RS3 (32 bits)
- Microsoft Windows 10 Mobile RS4 (32 bits)
- Microsoft Windows 10 Mobile Enterprise RS4 (32 bits)
- Microsoft Windows 10 Mobile RS5 (32 bits)
- Microsoft Windows 10 Mobile Enterprise RS5 (32 bits)
- Microsoft Windows 8 (Core) (32 bits o 64 bits)
- Microsoft Windows 7 Professional (32 bits o 64 bits)
- Microsoft Windows 7 Enterprise/Ultimate (32 bits o 64 bits)
- Microsoft Windows 7 Home Basic/Premium (32 bits o 64 bits)

- Microsoft Windows Vista Business con Service Pack 1 (32 bits o 64 bits)
- Microsoft Windows Vista Enterprise con Service Pack 1 (32 bits o 64 bits)
- Microsoft Windows Vista Ultimate con Service Pack 1 (32 bits o 64 bits)
- Microsoft Windows Vista Business con Service Pack 2 y versiones posteriores (32 bits o 64 bits)
- Microsoft Windows Vista Enterprise con Service Pack 2 y versiones posteriores (32 bits o 64 bits)
- Microsoft Windows Vista Ultimate con Service Pack 2 y versiones posteriores (32 bits o 64 bits)
- Microsoft Windows XP Professional con Service Pack 2 (32 bits o 64 bits)
- Microsoft Windows XP Home con Service Pack 3 y versiones posteriores de 32 bits
- Windows Essential Business Server 2008 Standard (64 bits)
- Windows Essential Business Server 2008 Premium (64 bits)
- Windows Small Business Server 2003 Standard con Service Pack 1 (32 bits)
- Windows Small Business Server 2003 Premium con Service Pack 1 (32 bits)
- Windows Small Business Server 2003 R2 Standard (32 bits)
- Windows Small Business Server 2003 R2 Premium (32 bits)
- Windows Small Business Server 2008 Standard (64 bits)
- Windows Small Business Server 2008 Premium (64 bits)
- Windows Small Business Server 2011 Standard (64 bits)
- Windows Small Business Server 2011 Premium Add-on (64 bits)
- Windows Small Business Server 2011 Essentials (64 bits)
- Windows Home Server 2011 (64 bits)
- Windows MultiPoint Server 2010 Standard (64 bits)
- Windows MultiPoint Server 2010 Premium (64 bits)
- Windows MultiPoint Server 2012 Standard/Premium (64 bits)
- Microsoft Windows 2000 Server (32 bits)
- Windows Server 2003 Enterprise con Service Pack 2 (32 bits o 64 bits)
- Windows Server 2003 Standard con Service Pack 2 (32 bits o 64 bits)
- Windows Server 2003 R2 Enterprise con Service Pack 2 (32 bits o 64 bits)
- Windows Server 2003 R2 Standard con Service Pack 2 (32 bits o 64 bits)

- Windows Server 2008 Datacenter con Service Pack 1 (32 bits o 64 bits)
- Windows Server 2008 Enterprise con Service Pack 1 (32 bits o 64 bits)
- Windows Server 2008 con Service Pack 1 Server Core (32 bits o 64 bits)
- Windows Server 2008 Standard con Service Pack 1 (32 bits o 64 bits)
- Windows Server 2008 Standard (32 bits o 64 bits)
- Windows Server 2008 Enterprise (32 bits o 64 bits)
- Windows Server 2008 Datacenter (32 bits o 64 bits)
- Windows Server 2008 R2 Server Core (64 bits)
- Windows Server 2008 R2 Datacenter (64 bits)
- Windows Server 2008 R2 Enterprise (64 bits)
- Windows Server 2008 R2 Foundation (64 bits)
- Windows Server 2008 R2 Standard (64 bits)
- Windows Server 2016 Nano (opción de instalación) (CBB)
- Windows Storage Server 2008 (32 bits o 64 bits)
- Windows Storage Server 2008 con Service Pack 2 (64 bits)
- Windows Storage Server 2008 R2 (64 bits)
- Windows Storage Server 2012 (64 bits)
- Windows Storage Server 2012 R2 (64 bits)
- Windows Storage Server 2016 (64 bits)
- Windows Storage Server 2019 (64 bits)
- Debian GNU/Linux 9.x (Stretch) (32 bits o 64 bits)
- Debian GNU/Linux 7.x (hasta la versión 7.8) (32 bits o 64 bits)
- Debian GNU/Linux 8.x (Jessie) (32 bits o 64 bits)
- Ubuntu Server 14.04 LTS (Trusty Tahr) (32 bits o 64 bits)
- Ubuntu Server 16.04 LTS (Xenial Xerus) (32 bits o 64 bits)
- Ubuntu Server 20.04.04 LTS (Focal Fossa) (ARM de 64 bits)
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) (32 bits o 64 bits)
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) (32 bits o 64 bits)

- Ubuntu Desktop 18.04 LTS (Bionic Beaver) (32 bits o 64 bits)
- Ubuntu Desktop 20.04 LTS (Focal Fossa) (32 bits o 64 bits)
- CentOS 6.x (hasta la versión 6.6) (64 bits)
- CentOS 7.x (ARM de 64 bits)
- CentOS 8.x (64 bits)
- SUSE Linux Enterprise Desktop 12 (todos los SP) (64 bits)
- SUSE Linux Enterprise Desktop 15, todos los Service Pack (64 bits)
- Astra Linux Special Edition 1.5 (64 bits)
- Astra Linux Special Edition RUSB.10265-01 (actualización operativa 8.1) Elbrus
- Astra Linux Special Edition RUSB.10015-16 (actualización operativa 8.1) Elbrus
- Pardus OS 19.1 (64 bits)
- Linux Mint 19.x (32 bits)
- Lotos (versión del núcleo Linux: 4.19.50; entorno de escritorio: MATE) (64 bits)
- ROSA Enterprise Linux Server 7.3 (64 bits)
- ROSA Enterprise Linux Desktop 7.3 (64 bits)
- ROSA COBALT Workstation 7.3 (64 bits)
- ROSA COBALT Server 7.3 (64 bits)

Las siguientes plataformas de virtualización son incompatibles:

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro

- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 (64 bits)
- Microsoft Hyper-V Server 2008 R2 (64 bits)
- Microsoft Hyper-V Server 2008 R2 con Service Pack 1 y posterior de 64 bits
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7

Kit de distribución

Puede adquirir la aplicación en las tiendas online de Kaspersky (por ejemplo, <https://www.kaspersky.es>) o a empresas asociadas.

Si compra Kaspersky Security Center Linux en una tienda en línea, tiene que bajar la aplicación del sitio web de esta. La información necesaria para la activación de la aplicación se le envía por correo electrónico tras la realización del pago.

Acerca de la compatibilidad del Servidor de administración y Kaspersky Security Center Web Console

Le recomendamos que utilice la última versión del Servidor de administración de Kaspersky Security Center Linux y de Kaspersky Security Center Web Console. De lo contrario, la funcionalidad de Kaspersky Security Center Linux puede verse limitada.

Puede instalar y actualizar el Servidor de administración de Kaspersky Security Center Linux y Kaspersky Security Center Web Console de forma independiente. Si lo hace, asegúrese de que la versión de Kaspersky Security Center Web Console instalada sea compatible con la versión del Servidor de administración al que busque conectarse:

- Web Console incluido en Kaspersky Security Center Linux 15 es compatible con las siguientes versiones del Servidor de administración de Kaspersky Security Center Linux: 15 y 14.2.
- El Servidor de administración incluido en Kaspersky Security Center Linux 15 es compatible con las siguientes versiones de Kaspersky Security Center Web Console: 15 y 14.2.

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. Esta Ayuda en línea contiene información sobre Kaspersky Security Center Linux. Para obtener información detallada sobre la solución basada en Windows, consulte la [Ayuda en línea de Kaspersky Security Center Windows](#).

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

Comparación de funciones de Kaspersky Security Center que funciona como una solución basada en Windows y una solución basada en Linux

Característica o propiedad	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15 Linux
Ubicación del Servidor de administración	Local	Local
Ubicación del sistema de administración de bases de datos (DBMS)	Local	Local
Sistema operativo para instalar el Servidor de administración en	Windows	Linux
Tipo de consola de administración	En las instalaciones y basado en la web	Basado en la web
Sistema operativo para instalar la consola de administración basada en web en	Windows o Linux	Linux
Jerarquía de Servidores de administración	✓	✓
Jerarquía de grupos de administración	✓	✓
Sondeo de red	✓	✓ (por rangos de IP y controladores de dominio, Samba 4 Active Directory, Microsoft Active Directory)
Número de dispositivos administrados	100 000	50 000 (con PostgreSQL y Postgres Pro)
Protección de dispositivos administrados: Windows, Linux y macOS	✓	✓
Protección de dispositivos móviles.	✓	—
Protección de máquinas virtuales	✓	✓
Protección de infraestructura de nube pública	✓	—
Administración de la seguridad centrada en el dispositivo	✓	✓
Gestión de seguridad centrada en el usuario	✓	✓

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	✓	✓
Actualización automática de las bases de datos antivirus	✓	✓
Compatibilidad con servidores de administración virtuales	✓	✓
Instalación de actualizaciones de software de terceros y reparación de vulnerabilidades de software de terceros	✓	— (usando solo una tarea de instalación remota)
Notificaciones sobre eventos ocurridos en dispositivos administrados	✓	✓
Creación y gestión de cuentas de usuario	✓	✓
Inicio de sesión en la consola mediante la autenticación del dominio	✓	✓ (El inicio de sesión único no es compatible con la versión actual)
Integración con sistemas SIEM	✓	✓ (solamente mediante el uso de Syslog)
Supervisión del estado de las directivas y tareas	✓	✓
Despliegue del clúster de conmutación por error de Kaspersky Security Center	✓	✓
Instalación del Servidor de administración en un clúster de conmutación por error de Windows Server	✓	—
Usar SNMP para enviar estadísticas del Servidor de administración a aplicaciones de terceros	✓	—
Diagnóstico remoto de dispositivos cliente	✓	✓
Conexión remota con el escritorio de un dispositivo cliente	✓	—
Administración de revisiones de objetos	✓	—
Actualización automática de las aplicaciones de Kaspersky	✓	—
Despliegue de sistemas operativos en dispositivos cliente	✓	—
Servidor web para publicar paquetes de instalación y otros archivos	✓	—
Visualización y trabajo con alertas detectadas por Kaspersky Endpoint Detection and Response Optimum	✓	✓

Uso del Servidor de administración como servidor WSUS	✓	—
Integración con Kaspersky Managed Detection and Response	✓	—
Compatibilidad con el control de anomalías adaptativo	✓	—
Compatibilidad con clústeres y conjuntos de servidores en grupos de administración	✓ (solo en Consola de administración basada en MMC)	✓
Administración de licencias de terceros	✓	—

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 o de la Web Console de Kaspersky Security Center.

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
- Español
- Español (Latinoamérica)

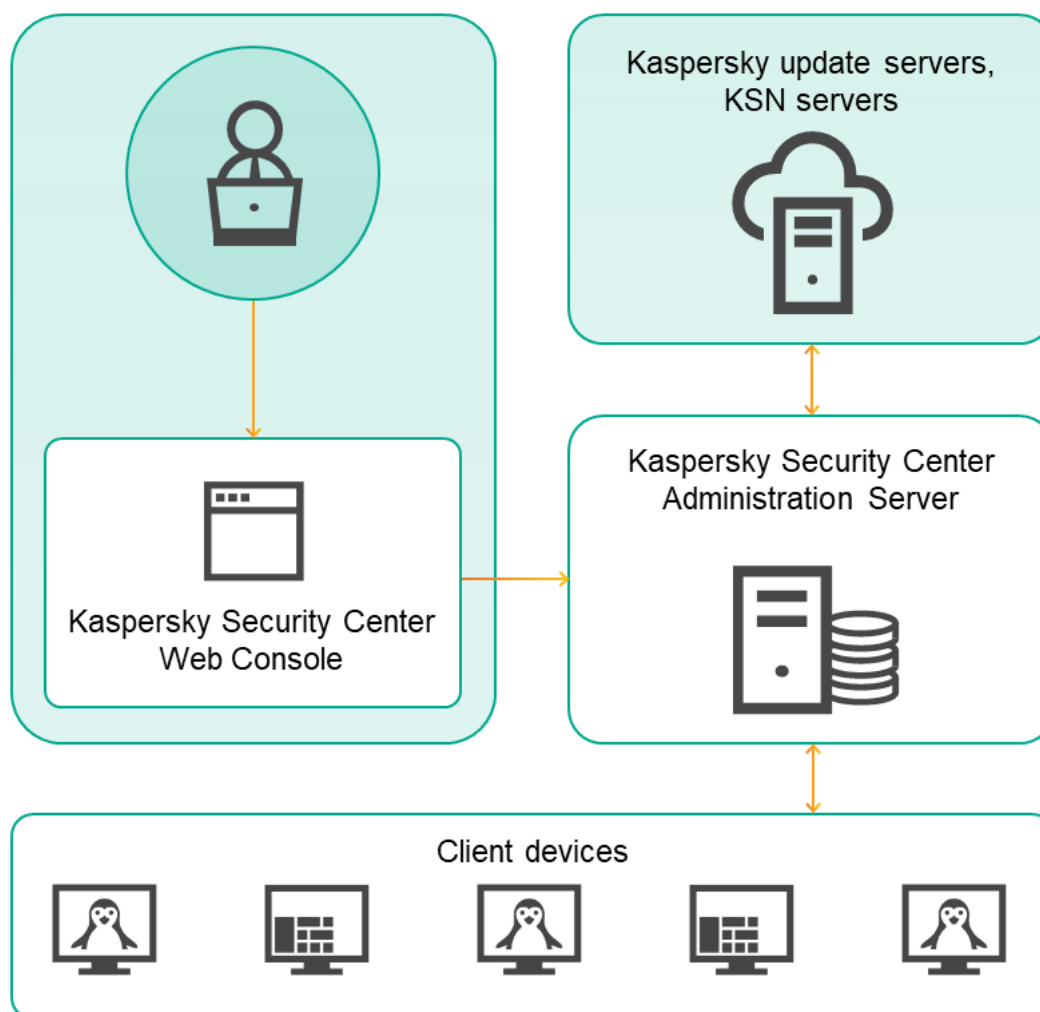
Puede obtener más información [sobre Kaspersky Security Center Cloud Console](#) y sus [características](#) en la [documentación de Kaspersky Security Center Cloud Console](#) y en la [documentación de Kaspersky Endpoint Security for Business](#).

Arquitectura y conceptos básicos

Esta sección explica la arquitectura y los conceptos básicos de la aplicación relacionados con Kaspersky Security Center Linux.

Arquitectura

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



Arquitectura de Kaspersky Security Center Linux

Kaspersky Security Center Linux contiene los siguientes componentes básicos:

- **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](#) garantiza respuestas más rápidas de las aplicaciones Kaspersky a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos.
- **Dispositivos cliente.** Dispositivos de la empresa cliente protegidos por Kaspersky Security Center Linux. Cada dispositivo que debe protegerse debe tener instalada una de las aplicaciones de seguridad de Kaspersky.

Diagrama de despliegue del Servidor de administración de Kaspersky Security Center Linux y Kaspersky Security Center Web Console

La siguiente figura muestra el diagrama de despliegue del Servidor de administración de Kaspersky Security Center Linux y Kaspersky Security Center Web Console.

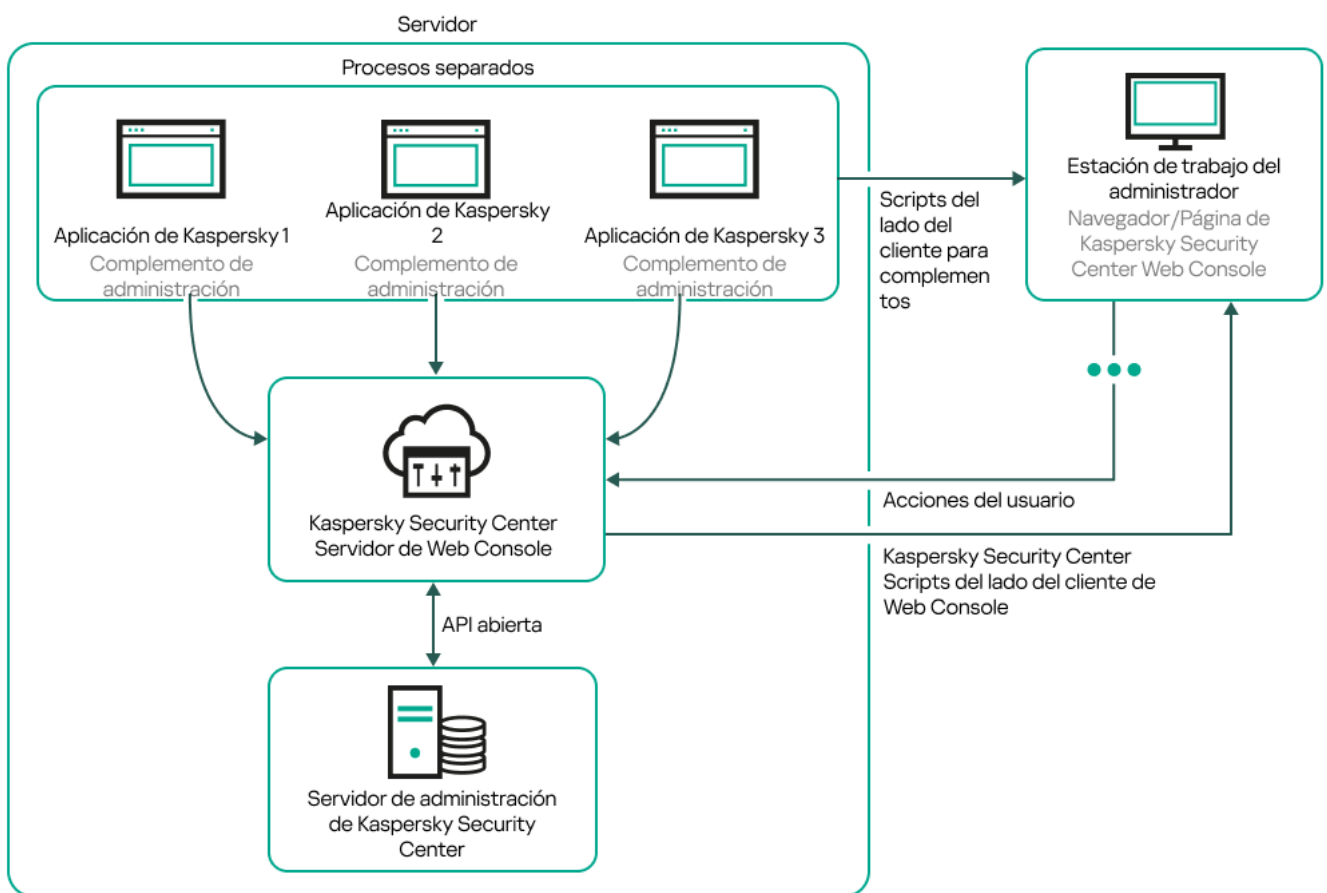


Diagrama de despliegue del Servidor de administración de Kaspersky Security Center Linux y Kaspersky Security Center Web Console

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 realiza acciones específicas en Kaspersky Security Center Web Console, Kaspersky Security Center de Web Console se comunica con el Servidor de administración de Kaspersky Security Center Linux a través de OpenAPI. El servidor de Kaspersky Security Center Web Console solicita la información requerida del Servidor de administración de Kaspersky Security Center Linux y muestra los resultados de sus operaciones en Kaspersky Security Center Web Console.

Puertos utilizados por Kaspersky Security Center Linux

Las siguientes tablas muestran los puertos predeterminados que deben estar abiertos en el Servidor de administración y en los dispositivos cliente. Si lo desea, puede cambiar cada uno de los números de puerto predeterminados.

Puerto utilizado por el Servidor de administración de Kaspersky Security Center Linux

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. Puede cambiar el número de puerto predeterminado en la sección Servidor web de la ventana de propiedades del Servidor de administración.
8061	klcsweb	TCP (TLS)	Transmisión de paquetes de instalación publicados a dispositivos cliente	Publicación de paquetes de instalación. Puede cambiar el número de puerto predeterminado en la sección Servidor web de la ventana de propiedades del Servidor de administración.
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. Puede cambiar el número del puerto predeterminado para recibir conexiones de los agentes de red al configurar los puertos de conexión durante la instalación de Kaspersky Security Center Linux; puede cambiar el número del puerto predeterminado para recibir conexiones de los servidores de administración secundarios al crear una jerarquía de servidores de administración .
13000	klserver	UDP	Recepción de información sobre dispositivos que se han apagado mediante los agentes de red	Administración de dispositivos cliente. Puede cambiar el número de puerto predeterminado en los ajustes de la directiva del Agente de red .
13299	klserver	TCP (TLS)	Recepción de conexiones de Kaspersky Security Center Web Console destinadas al Servidor de administración; recepción de conexiones para	Kaspersky Security Center Web Console, OpenAPI.

			el Servidor de administración realizadas mediante OpenAPI	Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración (en la subsección Puertos de conexión de la sección General), o al crear una jerarquía de Servidores de administración .
14000	klserver	TCP	Recepción de conexiones de los agentes de red	Administración de dispositivos cliente. Puede cambiar el número de puerto predeterminado al configurar puertos de conexión durante la instalación de Kaspersky Security Center Linux o al conectar manualmente un dispositivo cliente al Servidor de administración .
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. 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. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración .
17000	klactprx	TCP (TLS)	Recepción de conexiones para la activación de aplicaciones de dispositivos administrados	Activación del Servidor proxy para dispositivos administrados. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración (en la sección secundaria Puertos adicionales en la sección General).
19170	klserver	HTTPS (TLS)	Túneles de conexión establecidos con la utilidad klsc tunnel para comunicarse con los dispositivos administrados	Conexiones establecidas con dispositivos administrados remotos a través de Kaspersky Security Center Web Console. Puede cambiar el número de puerto predeterminado mediante la utilidad klsc flag.

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 donde se encuentra la base de datos (por ejemplo, el puerto 3306 para MariaDB). Consulte la documentación del DBMS para obtener la información necesaria.

La siguiente tabla muestra el puerto que debe estar abierto en 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.

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 a Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. Puede cambiar el número de puerto predeterminado al instalar Kaspersky Security Center Web Console . 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 debe estar abierto en los dispositivos administrados en los que se instaló 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	klagent	UDP	Señales de administración enviadas del Servidor de administración o del punto de distribución a los Agentes de red	Administración de dispositivos cliente. Puede cambiar el número de puerto predeterminado en los ajustes de la directiva del Agente de red .
15000	klagent	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	klagent	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. Puede cambiar el número de puerto predeterminado en la ventana propiedades del punto de distribución .

Tenga en cuenta que el proceso klagent 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 klagent en forma automática; por este motivo, el proceso klagent podría tomar puertos utilizados por otras aplicaciones. Si el proceso klagent 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.

Además, tenga en cuenta que las recomendaciones de compatibilidad de Kaspersky Security Center Linux con software de terceros solo se describen como referencia y es posible que no se puedan aplicar a las versiones nuevas de software de terceros. Las recomendaciones descritas para configurar los puertos se basan en las experiencias del Servicio de soporte técnico y en nuestras prácticas recomendadas.

La siguiente tabla muestra los puertos que deben estar abiertos en un dispositivo administrado que tiene instalado el Agente de red y que se designó como punto de distribución. Los puertos enumerados deben estar abiertos en 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	klagent	TCP (TLS)	Recepción de conexiones de Agentes de red y puertas de enlace de conexión	Administración de dispositivos cliente y distribución de actualizaciones y paquetes de instalación. Puede cambiar el número de puerto predeterminado en las propiedades del punto de distribución .
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. Puede cambiar el número de puerto predeterminado en las propiedades del punto de distribución .
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. Puede cambiar el número de puerto predeterminado en las propiedades del punto de distribución .

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	KSCWebConsolePlugin	HTTPS	Puerto de API que utilizan los procesos del complemento de administración para recibir solicitudes provenientes de KSCWebConsoleManagementService	Ejecución de procesos de nodo de complemento de administración
1329, 2003	KSCWebConsoleManagementService	HTTPS	Puertos de API que se utilizan para recibir las solicitudes de KSCWebConsoleManagementService, que se ejecuta en el mismo dispositivo	Actualización de los componentes de Kaspersky Security

				Cente Consc
2005	KSCWebConsole	HTTPS	Puerto de la API. Se utiliza para recibir las solicitudes del servicio KSCWebConsoleManagementService, que se ejecuta en el mismo dispositivo.	Ejecuc proce nodo Kaspe Secur Cente Consc
8200	—	HTTP	Puerto de la API. Se utiliza para generar certificados con HashiCorp Vault (para más información, visite el sitio web de HashiCorp Vault).	Instala Kaspe Secur Cente Consc actual de los comp de Kas Secur Cente Consc
4150, 4151, 4152	KSCWebConsoleMessageQueue	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	Intera entre Kaspe Secur Cente Consc compl de admin

Conceptos básicos

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

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 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 Linux, la aplicación muestra los nombres de los Servidores de administración que especificó como fiables en el [archivo de respuesta](#).

Puede conectarse al Servidor de administración mediante 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.

En una jerarquía, un Servidor de administración basado en Linux puede funcionar tanto como Servidor principal como Servidor secundario. El servidor principal basado en Linux puede administrar tanto servidores secundarios basados en Linux como basados en Windows. Un servidor principal basado en Windows puede administrar un servidor secundario basado en Linux.

[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.
- Uso de Kaspersky Security Center por parte de 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 varias organizaciones, un proveedor de servicios puede añadir Servidores de administración secundarios (incluidos Servidores 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 denominado *servidor virtual*) es un componente de Kaspersky Security Center Linux diseñado para administrar la protección antivirus 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).

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 no funciona correctamente, Kaspersky Security Center Linux 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 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 publicar paquetes de instalación independientes y archivos de una carpeta compartida a través de una carpeta compartida.

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.

La carpeta compartida se usa para el almacenamiento de información disponible para todos los usuarios cuyos dispositivos se administran mediante el 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:

- <nombre del Servidor web> es el nombre del Servidor web de Kaspersky Security Center.
- <puerto HTTPS> es un puerto HTTPS del Servidor web 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 el 8061.
- <objeto> es una subcarpeta o archivo al cual 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 se realiza mediante el componente *Agente de red* de Kaspersky Security Center Linux. El Agente de red se debe instalar en todos los dispositivos en los que Kaspersky Security Center Linux se utilice para administrar las aplicaciones de Kaspersky.

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

- Con el nombre "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*. Puede instalar el Agente de red 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

Cuando instala el Servidor de administración, la versión del servidor del Agente de red se instala automáticamente junto con el Servidor de administración. Sin embargo, para administrar el dispositivo del Servidor de administración como cualquier otro dispositivo administrado, [instale el Agente de red para Linux](#) en el dispositivo del Servidor de administración. En este caso, el Agente de red para Linux se instala y funciona independientemente de la versión del servidor del Agente de red que instaló junto con el Servidor de administración.

Los nombres de los procesos que el Agente de red inicia son los siguientes:

- klnagent64.service (para un sistema operativo de 64 bits)
- klnagent32.service (para un sistema operativo de 32 bits)

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* (en adelante *grupo*) es un conjunto lógico de dispositivos administrados combinados en función de un rasgo específico para la administración de dispositivos agrupados en una única unidad dentro de Kaspersky Security Center Linux.

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 equipo que utiliza esa persona del grupo de administración Contadores al grupo de administración Desarrolladores. Al efectivizarse el traspaso, el equipo recibirá automáticamente la configuración que los desarrolladores requieren para sus aplicaciones.

Dispositivo administrado

Un *dispositivo administrado* es un ordenador que ejecuta Linux y que tiene instalado Agente de red. 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 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 admitir hasta 20 000 dispositivos.

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

Los dispositivos que tienen instalado Kaspersky Security Center Web Console Server se denominan *estaciones de trabajo del administrador*. Los administradores pueden usar estos dispositivos para administrar en forma remota y centralizada las aplicaciones de Kaspersky instaladas en los dispositivos cliente.

No hay restricciones sobre el número de equipos administrador. En la red se pueden administrar simultáneamente grupos de administración de varios Servidores de administración desde cualquier estación de trabajo del administrador. 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 web de administración

Un componente especial, el *complemento web de administración*, se utiliza para la administración remota del software Kaspersky a través de Kaspersky Security Center Web Console. De aquí en adelante, un complemento web de administración se denomina también *complemento 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 la [Página web de soporte técnico 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 configuraciones de aplicaciones de Kaspersky que se aplican a 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 política tiene uno de los siguientes estados:

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.
- 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 produce 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 ayudarle a evitar la creación de varias instancias de una sola directiva, Kaspersky Security Center Linux le 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 Linux administra las aplicaciones de seguridad de Kaspersky instaladas en 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
- 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.

El administrador puede modificar las tareas locales mediante de Kaspersky Security Center Web Console o el usuario de un dispositivo remoto (por ejemplo, a través de la interfaz de la aplicación 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 Syslog y en el [registro de eventos de Kaspersky Security Center Linux](#), tanto de manera central en el Servidor de administración como de manera local 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.
Puede utilizar una dirección IP (o un rango IP) o un nombre DNS como la dirección del dispositivo.
- Importación de una lista de dispositivos desde un archivo .txt con las direcciones del dispositivo que se añadirán (cada dirección debe ubicarse en una línea individual).

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 la distribución de actualizaciones, la instalación remota de aplicaciones y la recuperación de información relativa a dispositivos en red. Un punto de distribución puede realizar las siguientes funciones:

- Distribuir las actualizaciones y los paquetes de instalación recibidos del Servidor de administración a los dispositivos cliente dentro del grupo (incluida la multidifusión a través de UDP). 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 aceleran la distribución de actualizaciones y liberan recursos en el Servidor de administración.

- 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.

Si no se puede establecer una conexión directa entre los dispositivos administrados del grupo y el Servidor de administración, se puede utilizar el punto de distribución como puerta de enlace de conexión al Servidor de administración para este grupo. 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.

- Sondar 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.
- Realice la instalación remota de aplicaciones de Kaspersky y de otros proveedores de software, incluida la instalación en dispositivos cliente sin 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 de proxy de KSN 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.

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 un perfil de conexión activo no participan en la detección de dominios de difusión.

Kaspersky Security Center Linux asigna a cada Agente de red una dirección IP de difusión múltiple única que se diferencia del resto de direcciones. Esto le permite evitar la sobrecarga de la red que podría ocurrir debido a superposiciones de IP. Las direcciones IP de difusión múltiple que se asignaron en versiones anteriores de la aplicación no se cambiarán.

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 de verificación 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 menor de 2 GB, Kaspersky Security Center Linux 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.

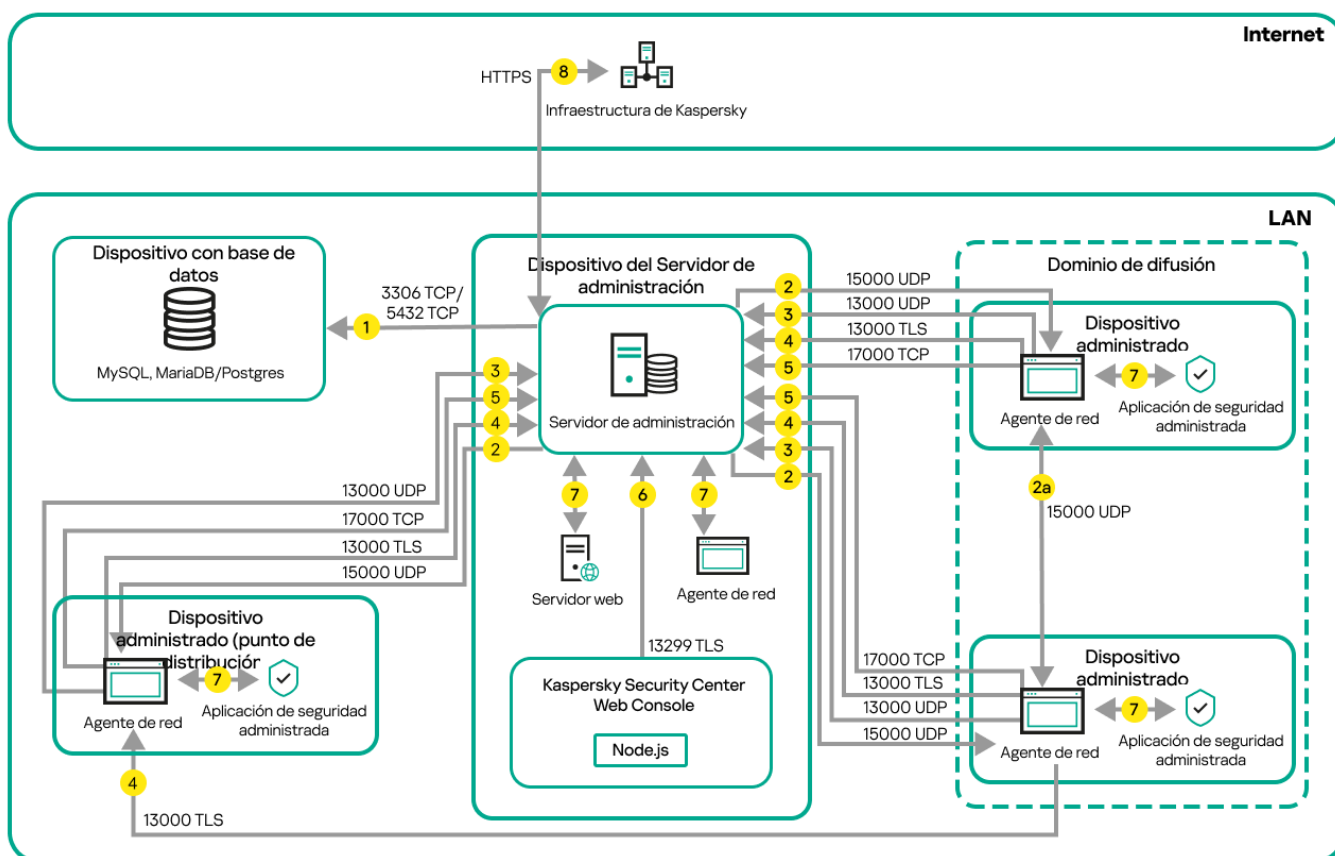
- También puede utilizar puertas de enlace de conexión dentro de la red. Por ejemplo, los puntos de distribución asignados automáticamente también se convierten en puertas de enlace de conexión en su propio ámbito. Sin embargo, dentro de una red interna, las puertas de enlace de conexión no brindan un 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.

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 Linux, 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 el 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 donde se encuentra la base de datos (por ejemplo, el puerto 3306 para un servidor MySQL o

MariaDB, o el puerto 5432 para un servidor PostgreSQL o Postgres Pro). 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 esos dispositivos no se envían directamente.

2a. Los Agentes de red en dispositivos administrados no móviles intercambian datos sobre otros Agentes de red dentro del mismo dominio de difusión (los datos se envían al Servidor de administración).

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 SSL 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 SSL) 14000. Kaspersky Security Center también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto SSL 13000.

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. 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.

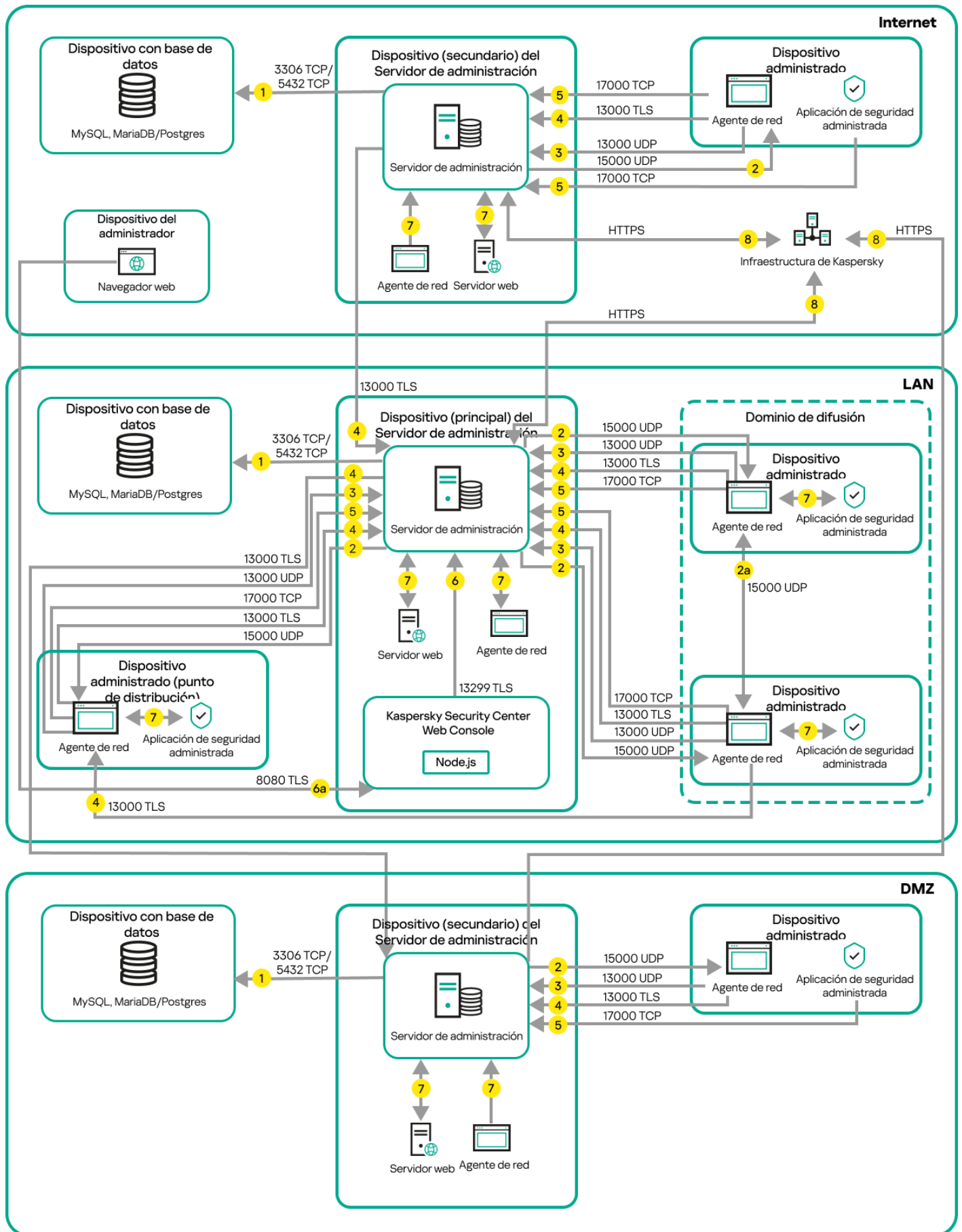
7. Las aplicaciones instaladas en un mismo dispositivo intercambian tráfico local (esto es válido tanto para el Servidor de administración como para los dispositivos administrados). No se deben abrir puertos externos.

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.

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 donde se encuentra la base de datos (por ejemplo, el puerto 3306 para un servidor MySQL o MariaDB, o el puerto 5432 para un servidor PostgreSQL o Postgres Pro). 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).

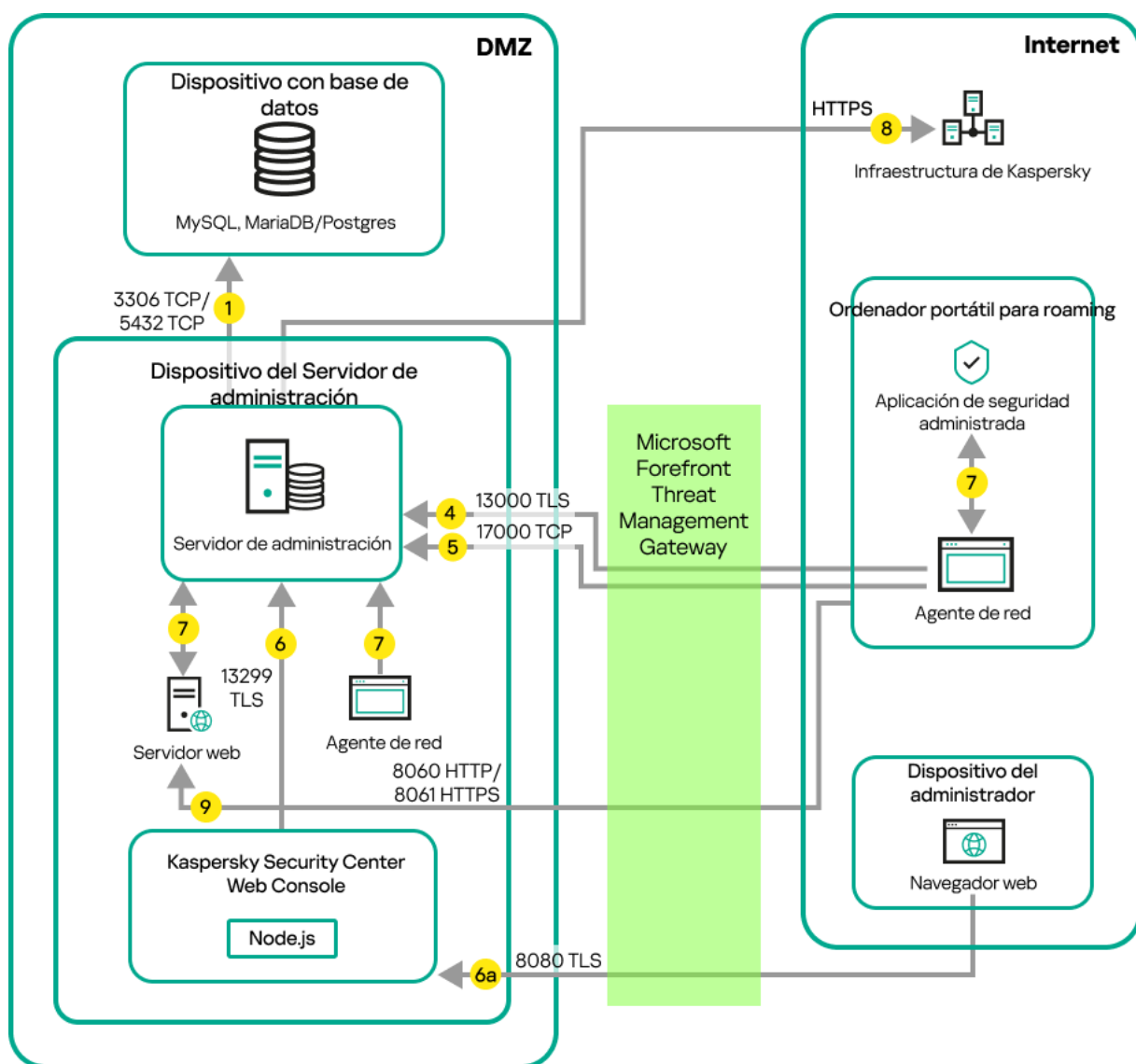
Si el Servidor de administración no tiene acceso directo a los dispositivos administrados, las solicitudes de comunicación del Servidor de administración a esos dispositivos no se envían directamente.
3. Cuando un dispositivo administrado se apaga, el Agente de red se lo comunica al Servidor de administración 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 SSL 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 SSL) 14000. Kaspersky Security Center Linux también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto SSL 13000.
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. 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.
 - 6a. 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.
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.

Servidor de administración en una LAN, dispositivos administrados en Internet, firewall en uso

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 están en Internet. En esta imagen, se utiliza el firewall corporativo que haya escogido. Consulte la documentación de la aplicación para obtener más detalles.



Servidor de administración en una red de área local; los dispositivos administrados se conectan al Servidor de administración a través de un firewall corporativo

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 donde se encuentra la base de datos (por ejemplo, el puerto 3306 para un servidor MySQL o MariaDB, o el puerto 5432 para un servidor PostgreSQL o Postgres Pro). 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).

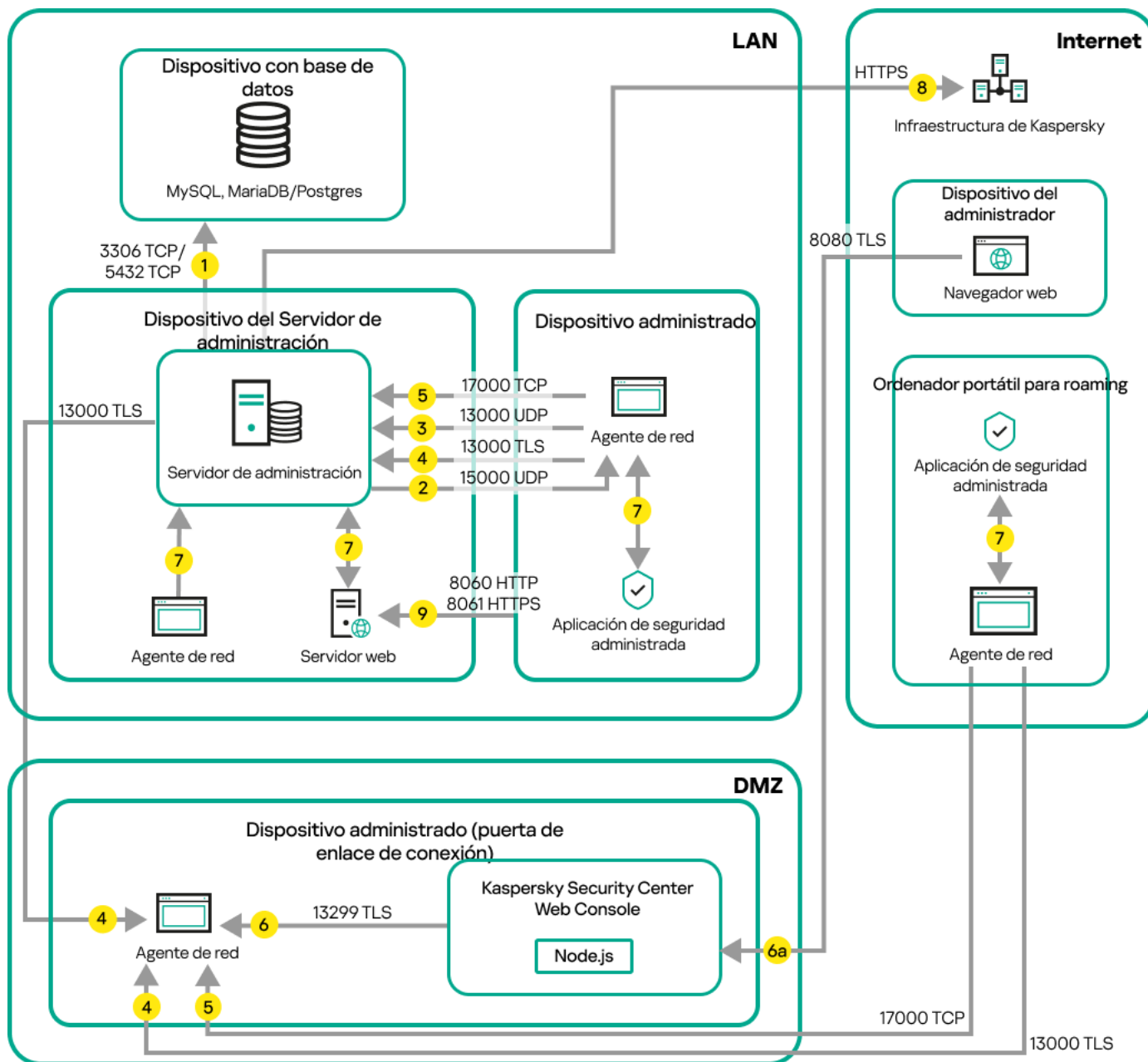
Si el Servidor de administración no tiene acceso directo a los dispositivos administrados, las solicitudes de comunicación del Servidor de administración a esos dispositivos no se envían directamente.

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 SSL 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 SSL) 14000. Kaspersky Security Center Linux también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto SSL 13000.
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. 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.
 - 6a. 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.
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. 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.

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 están en Internet. Se utiliza una puerta de enlace de conexión.

Se recomienda este esquema de despliegue si no desea que los dispositivos administrados se conecten directamente al Servidor de administración y no desea usar Microsoft Forefront Threat Management Gateway (TMG) 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 TMG 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 donde se encuentra la base de datos (por ejemplo, el puerto 3306 para un servidor MySQL o MariaDB, o el puerto 5432 para un servidor PostgreSQL o Postgres Pro). 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 esos dispositivos no se envían directamente.

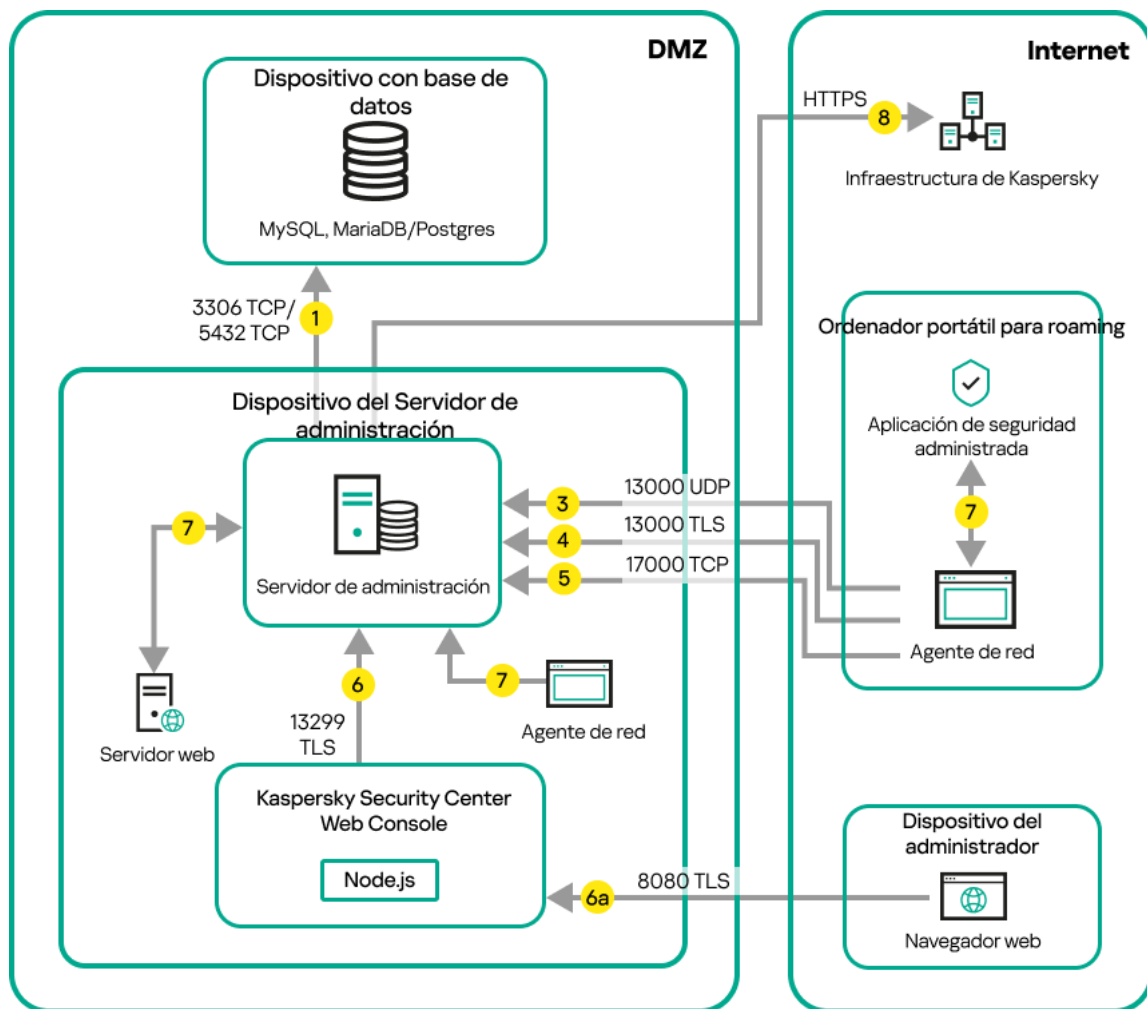
3. Cuando un dispositivo administrado se apaga, el Agente de red se lo comunica al Servidor de administración a través del puerto UDP 13000.
4. Los [Agentes de red](#) y los [Servidores de administración secundarios](#) se conectan con el Servidor de administración a través del puerto SSL 13000.

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 SSL) 14000. Kaspersky Security Center Linux también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto SSL 13000.
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. 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.
 - 6a. 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.
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. 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.

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 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 donde se encuentra la base de datos (por ejemplo, el puerto 3306 para un servidor MySQL o MariaDB, o el puerto 5432 para un servidor PostgreSQL o Postgres Pro). 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 esos 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 SSL 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 SSL) 14000. Kaspersky Security Center Linux también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto SSL 13000.

4a. Si existe una [puerta de enlace de conexión](#) en la DMZ, también recibe las conexiones del Servidor de administración a través del [puerto SSL 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 SSL 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. 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.

6a. 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.

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. Las solicitudes de paquetes de los dispositivos administrados se transfieren al [Servidor web](#), que se encuentra en el mismo dispositivo que el Servidor de administración.














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

Esta sección proporciona los esquemas para la interacción de componentes Kaspersky Security Center Linux 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

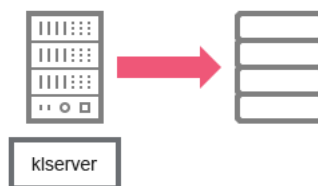
La siguiente tabla proporciona las convenciones usadas en los esquemas.

Convenciones del documento

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 Linux puede administrar)
	Puerta de enlace de conexión
	Punto de distribución
	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)
	Transporte de DBMS
	Límite de DMZ

Servidor de administración y DBMS

Los datos del Servidor de administración se introducen en una [base de datos](#).

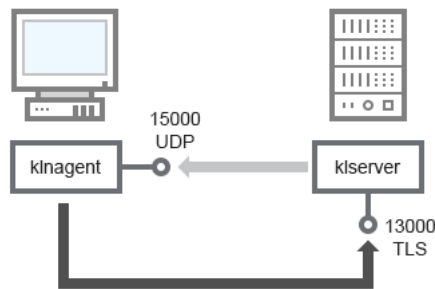


Servidor de administración y DBMS

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 donde se encuentra la base de datos (por ejemplo, el puerto 3306 para MariaDB). Consulte la documentación del DBMS para obtener la información necesaria.

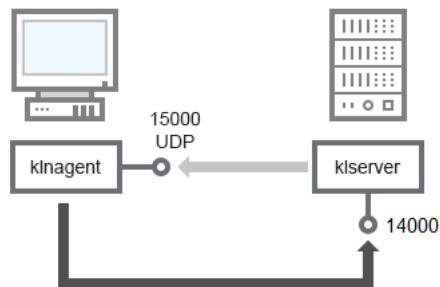
Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad

El Servidor de administración recibe la conexión de los Agentes de red a través del puerto TLS 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 Linux, 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 Linux 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)

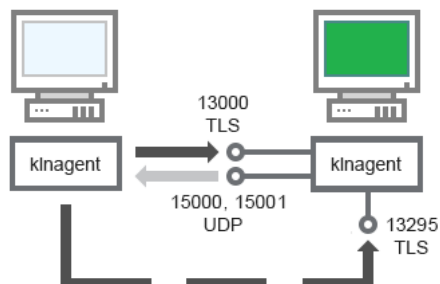
Para explicaciones sobre los esquemas, consulte la tabla a continuación.

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	Objetivo del puerto
Agente de red	15000	klnagent	UDP	Multidifusión para Agentes de red
Servidor de administración	13000	klserver	TCP (TLS)	Recepción de conexiones de los agentes de red
Servidor de administración	14000	klserver	TCP	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. La multidifusión del punto de distribución para Agentes de red se realiza mediante un 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.

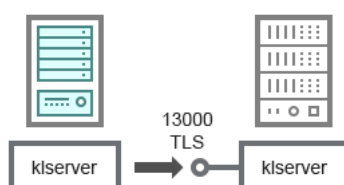
Actualización de software mediante un punto de distribución (tráfico)

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

Posteriormente, cuando los Servidores de administración se combinen en una jerarquía, podrá administrarlos mediante Kaspersky Security Center Web Console conectada al Servidor de administración principal. Por lo tanto, la accesibilidad del puerto 13299 del Servidor de administración principal es el único requisito previo.

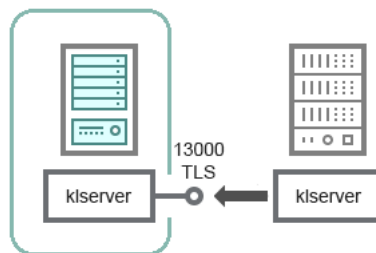


Para aclaraciones del esquema, consulte la tabla a continuación.

Jerarquía de Servidores de administración (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto
Servidor de administración principal	13000	klserver	TCP (TLS)	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

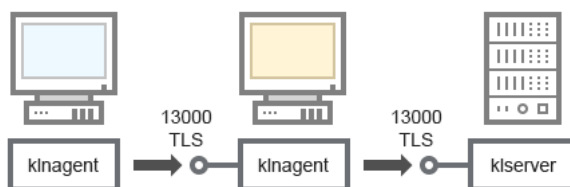
El esquema muestra una jerarquía de Servidores de administración en la que el Servidor de administración secundario ubicado en la "zona desmilitarizada" (DMZ) recibe una conexión del Servidor de administración principal (consulte la tabla a continuación para explicaciones sobre esquemas). Al combinar dos Servidores de administración en una jerarquía, asegúrese de que el puerto 13299 esté accesible en ambos Servidores de administración. Kaspersky Security Center Web Console está conectada a un Servidor de administración a través del puerto 13299.

Posteriormente, cuando los Servidores de administración se combinen en una jerarquía, podrá administrarlos mediante Kaspersky Security Center Web Console conectada al Servidor de administración principal. Por lo tanto, la accesibilidad del puerto 13299 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	Objetivo del puerto
Servidor de administración secundario	13000	klserver	TCP (TLS)	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



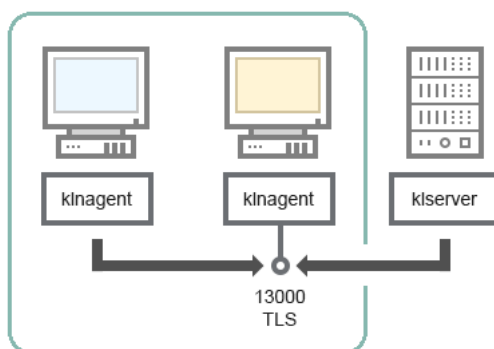
Servidor de administración, una puerta de enlace de conexión en un segmento de red y un dispositivo cliente

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	Objetivo del puerto
Servidor de administración	13000	klserver	TCP (TLS)	Recepción de conexiones de los agentes de red
Agente de red	13000	klnagent	TCP (TLS)	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



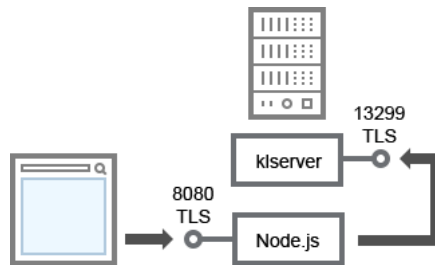
Servidor de administración con una puerta de enlace de conexión y un dispositivo cliente en DMZ

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	Objetivo del puerto
Agente de red	13000	klnagent	TCP (TLS)	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	Objetivo del puerto
Servidor de administración	13299	klserver	TCP (TLS)	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 (TLS)	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.

Primeros pasos

Siguiendo estas instrucciones, puede instalar el Servidor de administración de Kaspersky Security Center Linux y 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.

Requisitos previos

Debe tener una clave de licencia (código de activación) para Kaspersky Security Center for Business o claves de licencia (códigos de activación) para las aplicaciones de seguridad de Kaspersky.

Si primero desea probar Kaspersky Security Center Linux, puede obtener una prueba gratuita de 30 días en el [sitio web de Kaspersky](#).

Etapas

El escenario de instalación principal se desarrolla en etapas:

1 Selección de una estructura para la protección de organización

[Más información sobre los componentes de Kaspersky Security Center Linux](#). 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).

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.

2 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](#).

3 Instalación de un sistema de gestión de bases de datos (DBMS)

Instale el DBMS que utilizará Kaspersky Security Center Linux o utilice uno existente.

Puede elegir una de las [DBMS admitidas](#). Para obtener información sobre cómo instalar el DBMS seleccionado, consulte su documentación.

Si la distribución de su sistema operativo basado en Linux no contiene un DBMS compatible, puede instalar el DBMS desde un repositorio de paquetes de terceros. Si la instalación de distribuciones desde repositorios de terceros está prohibida, puede instalar el DBMS en un dispositivo aparte.

Si decide instalar PostgreSQL o Postgres Pro DBMS, asegúrese de haber especificado 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.

Si instala [MariaDB](#), [PostgreSQL](#), o [Postgres Pro](#), use la configuración recomendada para garantizar que el DBMS funcione correctamente.

Si desea cambiar el [tipo de DBMS](#) después de la instalación, debe reinstalar Kaspersky Security Center Linux. Los datos se pueden transferir parcial y manualmente a otra base de datos.

4 Configure los puertos

Asegúrese de que todos los [puertos](#) necesarios estén abiertos para la interacción entre los componentes de acuerdo con la estructura de seguridad que haya seleccionado.

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.

5 Instalación de Kaspersky Security Center Linux

Seleccione un dispositivo Linux que desee utilizar como Servidor de administración, asegúrese de que el dispositivo cumpla con los [requisitos de software y hardware](#), y entonces [instale Kaspersky Security Center Linux](#) en el dispositivo. La versión de servidor del Agente de red se instala automáticamente junto con el Servidor de administración.

6 Instalar Kaspersky Security Center Web Console y complementos de administración

Seleccione un dispositivo Linux que desee utilizar como estación de trabajo del administrador, asegúrese de que el dispositivo cumpla con los [requisitos de software y hardware](#) y luego instale Kaspersky Security Center Web Console en el dispositivo. Puede instalar Kaspersky Security Center Web Console en el mismo dispositivo donde está instalado el Servidor de administración o en uno diferente.

[Descargue el complemento web de administración de Kaspersky Endpoint Security for Linux](#) y luego instálelo en el mismo dispositivo donde está instalado Kaspersky Security Center Web Console.

7 Instalar Kaspersky Endpoint Security para Linux y el Agente de red en el dispositivo del Servidor de administración

De manera predeterminada, la aplicación no considera el dispositivo del Servidor de administración como un dispositivo administrado. Para proteger el Servidor de administración contra virus y otras amenazas, y para administrar el dispositivo como cualquier otro dispositivo administrado, le recomendamos que [instale Kaspersky Endpoint Security for Linux](#) y [Agente de red para Linux](#) en el dispositivo del Servidor de administración. En este caso, el Agente de red para Linux se instala y funciona independientemente de la versión del servidor del Agente de red que instaló junto con el Servidor de administración.

8 Realizar la configuración inicial

Cuando la instalación del Servidor de administración se completa, en la primera conexión con el Servidor de administración, el [asistente de inicio rápido](#) comienza automáticamente. Realice la configuración inicial del Servidor de administración según los requisitos existentes. Durante la etapa de configuración inicial, el asistente usa la configuración predeterminada para crear las [directivas](#) y las [tareas](#) que son necesarias para desplegar la protección. Sin embargo, las configuraciones predeterminadas pueden ser menos que óptimas para las necesidades de su organización. Puede [cambiar la configuración de directivas y tareas](#) si es necesario.

9 Detección de dispositivos de red

Detecte los dispositivos manualmente. Kaspersky Security Center Linux recibe las direcciones y los nombres de todos los dispositivos detectados en la red. A continuación, puede usar Kaspersky Security Center Linux para instalar aplicaciones y software de Kaspersky desde otros proveedores en los dispositivos detectados. Cada cierto tiempo, Kaspersky Security Center Linux inicia una detección de dispositivos, lo que significa que si aparece alguna instancia nueva en la red, se la detectará automáticamente.

10 Organización de dispositivos en grupos de administración

En algunos casos, para desplegar la protección en dispositivos en red de la forma más cómoda puede ser necesario [dividir el conjunto completo de dispositivos en grupos de administración](#), tomando en cuenta la estructura de la organización. Puede crear [reglas de movimiento para distribuir dispositivos entre grupos](#) o puede distribuir 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 de que ya no haya dispositivos no asignados en la red.

11 Designar los puntos de distribución

Los [puntos de distribución](#) se asignan automáticamente a los grupos de administración, pero también 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.

12 Instalación del Agente de red y aplicaciones de seguridad en dispositivos en red

La implementación de protección en una red empresarial implica la [instalación del Agente de red y aplicaciones de seguridad](#) en dispositivos que el Servidor de administración ha detectado durante la detección 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).

13 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.

14 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 y/o la administración de seguridad centrada en el usuario. 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](#).

15 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 Linux y Kaspersky Security Center Web Console.

Configurar el servidor MariaDB x64 para trabajar con Kaspersky Security Center Linux

Configuración recomendada para el archivo my.cnf

Para obtener más detalles sobre la configuración de DBMS, consulte también el procedimiento de [configuración de la cuenta](#). Para obtener información sobre la instalación de DBMS, consulte el procedimiento de [instalación de DBMS](#).

Para configurar el archivo my.cnf:

1. [Abra el archivo my.cnf](#) en un editor de textos.
2. Añada las siguientes líneas en la sección [mysqld] del archivo my.cnf:

```
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=< valor >
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
```

El valor de `innodb_buffer_pool_size` no debe ser inferior al 80 % del tamaño previsto 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 usar el valor del parámetro `innodb_flush_log_at_trx_commit=0`, debido a que los valores "1" o "2" afectan de modo negativo la velocidad operativa de MariaDB.

De forma predeterminada, los complementos del optimizador `join_cache_incremental`, `join_cache_hashed`, y `join_cache_bka` están activados. 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`, entonces los complementos del optimizador están activados.

Si estas líneas faltan o tienen el valor `off`, haga lo siguiente:

- a. Abra el archivo `my.cnf` en un editor de textos.

- b. Añada las siguientes líneas al archivo `my.cnf`:

```
optimizer_switch='join_cache_incremental=on'
optimizer_switch='join_cache_hashed=on'
optimizer_switch='join_cache_bka=on'
```

Están habilitados los complementos `join_cache_incremental`, `join_cache_hash` y `join_cache_bka`.

Configurar el servidor PostgreSQL o Postgres Pro para trabajar con Kaspersky Security Center Linux

Kaspersky Security Center Linux es compatible con PostgreSQL y Postgres Pro DBMS. Si usa uno de estos DBMS, plantéese configurar los parámetros del servidor DBMS para optimizar el funcionamiento del DBMS con Kaspersky Security Center Linux.

La ruta predeterminada al archivo de configuración es: `/etc/postgresql/<VERSION>/main/postgresql.conf`

Parámetros recomendados para PostgreSQL y Postgres Pro:

- `shared_buffers` = 25 % del valor de RAM del dispositivo en el que está instalado el DBMS
Si la memoria RAM es inferior a 1 GB, deje el valor predeterminado.
- `max_stack_depth` = tamaño máximo de la pila (ejecute el comando "`ulimit -s`" para obtener este valor en KB) menos el margen de seguridad de 1 MB
- `temp_buffers` = 24 MB
- `work_mem` = 16 MB
- `max_connections` = 151
- `max_parallel_workers_per_gather` = 0
- `maintenance_work_mem` = 128 MB

Reinicie o vuelva a cargar el servidor después de actualizar el archivo `postgresql.conf` para aplicar los cambios. Consulte la [documentación de PostgreSQL](#) para obtener más detalles.

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](#).

Para obtener información detallada sobre los parámetros del servidor PostgreSQL y Postgres Pro y sobre cómo especificar los parámetros, consulte la documentación DBMS correspondiente.

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. Utilice un certificado de una CA de confianza porque un certificado autofirmado solo proporciona protección limitada.

El Servidor de administración es compatible con la autenticación SSL unidireccional y bidireccional de PostgreSQL.

Siga estos pasos para configurar la autenticación SSL de PostgreSQL:

1 Genere un certificado para el servidor PostgreSQL.

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 Genere 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. De manera predeterminada, el nombre de usuario configurado es postgres.

```
openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -subj "/CN=postgres"
```

```
chmod og-rwx postgres.key
```

3 Configure la autenticación del certificado 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 Especifique 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 = '*'
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 = '*'
ssl = on
ssl_ca_file = '<postgres.crt>'
ssl_cert_file = '<psql.crt>'
ssl_key_file = '<psql.key>'
```

5 Reinicie el demonio PostgreSQL.

Ejecute el siguiente comando:

```
systemctl restart postgresql-14.service
```

6 Especifique el indicador de servidor para el Servidor de administración.

[Autenticación SSL unidireccional](#)

Navegue hasta el directorio ServerFlags y cree un archivo que corresponda al indicador de servidor KLSRV_POSTGRES_OPT_SSL_CA:

```
cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/  
mkfile KLSRV_POSTGRES_OPT_SSL_CA
```

En el archivo creado, especifique la ruta al archivo psql.crt.

Autenticación SSL bidireccional

Navegue hasta el directorio ServerFlags y cree archivos que correspondan a los indicadores de servidor:

```
cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/  
mkfile KLSRV_POSTGRES_OPT_SSL_CA  
mkfile KLSRV_POSTGRES_OPT_SSL_CERT  
mkfile KLSRV_POSTGRES_OPT_SSL_KEY
```

Edite los archivos creados de la siguiente manera:

- KLSRV_POSTGRES_OPT_SSL_CA: especifique la ruta al archivo psql.crt.
- KLSRV_POSTGRES_OPT_SSL_CERT: especifique la ruta al archivo postgres.crt.
- KLSRV_POSTGRES_OPT_SSL_KEY: especifique la ruta al archivo postgres.key.

Si postgres.key requiere una contraseña, cree un archivo KLSRV_POSTGRES_OPT_TLS_PASPHRASE en la carpeta ServerFlags y especifique la contraseña en él.

Reinicie el servicio del Servidor de administración.

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. Utilice un certificado de una CA de confianza porque un certificado autofirmado solo proporciona protección limitada.

El Servidor de administración es compatible con la autenticación SSL unidireccional y bidireccional de MySQL.

Activación de la autenticación SSL unidireccional

Siga estos pasos para configurar la autenticación SSL unidireccional de MySQL:

1. Navegue hasta el directorio ServerFlags y cree un archivo que corresponda al indicador de servidor KLSRV_MYSQL_OPT_SSL_CA:

```
cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/  
mkfile KLSRV_MYSQL_OPT_SSL_CA
```

2. En el archivo KLSRV_MYSQL_OPT_SSL_CA, especifique la ruta al certificado (el archivo ca-cert.pem).

3. Especifique los certificados en el archivo my.cnf. Abra el archivo my.cnf en un editor de texto y añada las siguientes líneas en la sección [mysqld]:

```
[mysqld]
ssl-ca="C:/mysqlCerts/ca-cert.pem"
ssl-cert="C:/mysqlCerts/server-cert.pem"
ssl-key="C:/mysqlCerts/server-key.pem"
```

Activación de la autenticación SSL bidireccional

Siga estos pasos para configurar la autenticación SSL bidireccional de MySQL:

1. Navegue hasta el directorio ServerFlags y cree archivos que correspondan a los indicadores de servidor:

```
cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/
mkfile KLSRV_MYSQL_OPT_SSL_CA
mkfile KLSRV_MYSQL_OPT_SSL_CERT
mkfile KLSRV_MYSQL_OPT_SSL_KEY
```

2. Edite los archivos creados de la siguiente manera:

KLSRV_MYSQL_OPT_SSL_CA: especifique la ruta al archivo ca-cert.pem.

KLSRV_MYSQL_OPT_SSL_CERT: especifique la ruta al archivo server-cert.pem.

KLSRV_MYSQL_OPT_SSL_KEY: especifique la ruta al archivo server-key.pem.

Si server-key.pem requiere una frase de contraseña, cree un archivo KLSRV_MARIADB_OPT_TLS_PASPHRASE en la carpeta ServerFlags y especifique la frase de contraseña en él.

3. Especifique los certificados en el archivo my.cnf. Abra el archivo my.cnf en un editor de texto y añada las siguientes líneas en la sección [mysqld]:

```
[mysqld]
ssl-ca="C:/mysqlCerts/ca-cert.pem"
ssl-cert="C:/mysqlCerts/server-cert.pem"
ssl-key="C:/mysqlCerts/server-key.pem"
```

Instalación de Kaspersky Security Center Linux

Este procedimiento describe cómo instalar Kaspersky Security Center Linux.

Antes de la instalación:

- [Instale un DBMS.](#)
- Asegúrese de que el dispositivo donde desea instalar Kaspersky Security Center Linux esté ejecutando una de las [distribuciones de Linux compatibles.](#)

Utilice el archivo de instalación — ksc64_[version_number]_amd64.deb o ksc64-[version_number].x86_64.rpm — que corresponda a la distribución de Linux instalada en su dispositivo. El archivo de instalación debe descargarse del sitio web de Kaspersky.

Para instalar Kaspersky Security Center Linux:

1. En la línea de comandos, ejecute los comandos provistos en esta instrucción bajo una cuenta con privilegios de raíz.
2. Cree un grupo 'kldadmins' y una cuenta sin privilegios 'ksc'. La cuenta debe ser miembro del grupo 'kldadmins'. Para hacer esto, ejecute los siguientes comandos en secuencia:

```
# adduser ksc
# groupadd kldadmins
# gpasswd -a ksc kldadmins
# usermod -g kldadmins ksc
```
3. Ejecute la instalación de Kaspersky Security Center Linux. Según su distribución de Linux, ejecute uno de los siguientes comandos:
 - # apt install /<path>/ksc64-[version_number]_amd64.deb
 - # yum install /<path>/ksc64-[version_number].x86_64.rpm -y
4. Ejecute la configuración de Kaspersky Security Center Linux:

```
# /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```
5. Lea el [Contrato de licencia de usuario final](#) (EULA) y la Política de privacidad. 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 lo solicite, ingrese los siguientes valores:
 - a. Ingrese y si entiende y acepta los términos del EULA. Ingrese n si no acepta los términos del EULA. Para usar Kaspersky Security Center Linux, debe aceptar las condiciones del EULA.
 - b. Ingresar y si comprende y acepta los términos de la Política de privacidad, y acepta que sus datos se manejarán y transmitirán (incluso a terceros países) como se describe en la Política de privacidad. Ingresar n si no acepta los términos de la Política de privacidad. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos de la Política de privacidad.
6. Cuando se lo solicite, ingrese los siguientes ajustes:
 - a. Introduzca el nombre DNS o la dirección IP estática del Servidor de administración. 127.0.0.1 para una instalación de base de datos local.
 - b. Introduzca el número de puerto SSL del Servidor de administración. De manera predeterminada, se utiliza el puerto 13000.
 - c. Evalúe el número aproximado de dispositivos que desea administrar:
 - Si tiene de 1 a 100 dispositivos en red, ingrese 1.
 - Si tiene de 101 a 1000 dispositivos en red, ingrese 2.
 - Si tiene más de 1000 dispositivos en red, ingrese 3.
 - d. Ingrese el nombre del grupo de seguridad para los servicios. De forma predeterminada, se utiliza el grupo kldadmins.
 - e. Introduzca el nombre de la cuenta para iniciar el servicio del Servidor de administración. La cuenta debe ser miembro del grupo de seguridad ingresado. De forma predeterminada, se utiliza la cuenta ksc.
 - f. Introduzca el nombre de la cuenta para iniciar otros servicios. La cuenta debe ser miembro del grupo de seguridad ingresado. De forma predeterminada, se utiliza la cuenta ksc.

g. Seleccione el DBMS que instaló para trabajar con Kaspersky Security Center Linux:

- Si instaló MySQL o MariaDB, introduzca 1.
- Si instaló PostgreSQL o Postgres Pro, ingrese 2.

h. Introduzca el nombre de DNS o la dirección IP del dispositivo en el que está instalada la base de datos.
127.0.0.1 para la instalación de una base de datos local.

i. Introduzca el número de puerto de la base de datos. Este puerto se utiliza para comunicarse con el Servidor de administración. De forma predeterminada, se utilizan los siguientes puertos:

- Puerto 3306 para MySQL o MariaDB
- Puerto 5432 para PostgreSQL o Postgres Pro

j. Introduzca el nombre de la base de datos.

k. Introduzca el inicio de sesión de la cuenta root de la base de datos que utiliza para acceder a la base de datos.

l. Introduzca la contraseña de la cuenta root de la base de datos que utiliza para acceder a la base de datos.
Espere a que los servicios se añadan e inicien automáticamente:

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

m. Cree una cuenta que actuará como administrador del Servidor de administración. Introduzca el nombre de usuario y la contraseña. Puede usar el siguiente comando para crear un nuevo usuario:
`/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <contraseña>`

La contraseña debe cumplir con las siguientes reglas:

- La contraseña de usuario no puede tener menos de 8 ni más de 16 caracteres.
- La contraseña debe contener caracteres de al menos tres de los grupos enumerados a continuación:
 - Letras mayúsculas (A-Z)
 - Letras minúsculas (a-z)
 - Números (0-9)
 - Caracteres especiales (@ # \$ % ^ & * - _ ! + = [] { } | : ' . ? / \ ` ~ " () ;)

El usuario se añade y se instala Kaspersky Security Center Linux.

Verificación del servicio

Use los siguientes comandos para verificar si un servicio se está ejecutando o no:

- # systemctl status klagent_srv.service
- # systemctl status kladminserver_srv.service
- # systemctl status klactprx_srv.service
- # systemctl status klwebsrv_srv.service

Instalación de Kaspersky Security Center Linux en modo silencioso

Puede instalar Kaspersky Security Center Linux en dispositivos Linux mediante el uso de un archivo de respuesta para ejecutar una instalación en modo silencioso; es decir, sin la participación del usuario. El archivo de respuesta contiene un conjunto personalizado de parámetros de instalación: variables y sus respectivos valores.

Antes de la instalación:

- Instale un [sistema de gestión de bases de datos \(DBMS\)](#).
- Asegúrese de que el dispositivo donde desea instalar Kaspersky Security Center Linux esté ejecutando una de las [distribuciones de Linux compatibles](#).

Para instalar Kaspersky Security Center Linux en modo silencioso, siga estos pasos:

1. 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.

2. Cree un grupo 'kladmins' y una cuenta sin privilegios 'ksc', que debe ser miembro del grupo 'kladmins'. Para hacerlo, ejecute secuencialmente los siguientes comandos en una cuenta con privilegios root:

```
# adduser ksc
# groupadd kladmins
# gpasswd -a ksc kladmins
# usermod -g kladmins ksc
```

3. Cree el archivo de respuesta (en formato TXT) y añada una lista de variables en el formato VARIABLE_NAME=variable_value al archivo de respuesta, cada una en una línea separada. El archivo de respuesta debe incluir las variables enumeradas en la tabla a continuación.

4. Establezca el valor de la variable de entorno KLAUTOANSWERS en el entorno raíz que contiene el nombre completo del archivo de respuesta, incluida la ruta; por ejemplo, con el siguiente comando:

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

5. Ejecute la instalación de Kaspersky Security Center Linux en modo silencioso; según la distribución de Linux, ejecute uno de los siguientes comandos:

- # apt install /<path>/ksc64_[version_number]_amd64.deb
- # yum install /<path>/ksc64-[version_number].x86_64.rpm -y

6. Cree un usuario para trabajar con Kaspersky Security Center Web Console. Para hacerlo, ejecute el siguiente comando bajo una cuenta con privilegios root:

```
/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p < contraseña >, donde la contraseña debe contener al menos 8 caracteres.
```

Variables del archivo de respuesta utilizadas como parámetros de instalación de Kaspersky Security Center Linux en modo silencioso

Nombre de la variable	Obligatoria	Descripción	Valores
EULA_ACCEPTED	Sí	Confirme que entiende y acepta los términos del Contrato de licencia de usuario final.	1
PP_ACCEPTED	Sí	Confirme que entiende y acepta los términos de la Política de privacidad.	1
KLSRV_UNATT_SERVERADDRESS	Sí	El nombre DNS o la dirección IP estática del Servidor de administración.	Nombre DNS o IP
KLSRV_UNATT_PORT_SRV	No	El número de puerto del Servidor de administración. Opcional. El valor predeterminado es 14000.	Número de puerto
KLSRV_UNATT_PORT_SRV_SSL	No	El número de puerto SSL del Servidor de administración. Opcional. El valor predeterminado es 13000.	Número de puerto
KLSRV_UNATT_PORT_KLOAPI	No	El número de puerto KLOAPI del Servidor de administración. Opcional. El valor predeterminado es 13299.	Número de puerto
KLSRV_UNATT_PORT_GUI	No	El número de puerto de la GUI del Servidor de administración. Opcional. El valor predeterminado es 13291.	Número de puerto
KLSRV_UNATT_NETRANGETYPE	No	El número aproximado de dispositivos que desea administrar. Opcional. El valor predeterminado es 1.	1 para 1 a 10 en red. 2 para 101 a 1000 dispositivos 3 para más dispositivos
KLSRV_UNATT_DBMS_TYPE	Sí	El tipo de sistema de administración de bases de datos: MySQL (MariaDB) o Postgres.	mysql o postgres
KLSRV_UNATT_DBMS_INSTANCE	Sí	La dirección IP del servidor de la base de datos.	Dirección IP
KLSRV_UNATT_DBMS_PORT	Sí	El puerto del servidor de la base de datos. El valor predeterminado para MySQL (MariaDB) es 3306; el valor predeterminado para Postgres es 5432.	3306 o 5432
KLSRV_UNATT_DB_NAME	Sí	El nombre de la base de datos.	kav
KLSRV_UNATT_DBMS_LOGIN	Sí	El nombre de usuario de un usuario que tiene acceso a la base de datos.	
KLSRV_UNATT_DBMS_PASSWORD	Sí	La contraseña de un usuario que tiene acceso a la base de datos.	

KLSRV_UNATT_KLADMINSGROUP	Sí	El nombre del grupo de seguridad para los servicios.	kladmins
KLSRV_UNATT_KLSRVUSER	Sí	El nombre de la cuenta para iniciar el servicio del Servidor de administración. La cuenta debe ser miembro del grupo de seguridad especificado en la variable KLSRV_UNATT_KLADMINSGROUP.	ksc
KLSRV_UNATT_KLSVCUSER	Sí	El nombre de la cuenta para iniciar otros servicios. La cuenta debe ser miembro del grupo de seguridad especificado en la variable KLSRV_UNATT_KLADMINSGROUP.	ksc

Si el Servidor de administración se despliega como un [clúster de conmutación por error de Kaspersky Security Linux](#), el archivo de respuesta debe incluir las siguientes variables adicionales:

KLFOC_UNATT_NODE	Sí	El número de nodo (1 o 2).	1 o 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	Sí	El punto de montaje de la carpeta compartida de estados.	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	Sí	El punto de montaje de la carpeta compartida de datos.	
KLFOC_UNATT_CONN_MODE	Sí	El modo de conectividad del clúster de conmutación por error.	VirtualAd. o ExternalL

En caso de que la variable KLFOC_UNATT_CONN_MODE tenga el valor VirtualAdapter, el archivo de respuesta debe incluir las siguientes variables adicionales:

KLFOC_UNATT_CONN_MODE_VA_NAME		El nombre del adaptador de red virtual.	
KLFOC_UNATT_CONN_MODE_VA_IPV4	Se requiere una de estas variables	La dirección IP del adaptador de red virtual.	Dirección IP
KLFOC_UNATT_CONN_MODE_VA_IPV6		La dirección IPv6 del adaptador de red virtual.	Dirección IP

Instalación de Kaspersky Security Center Linux en Astra Linux en el modo de entorno de software cerrado

En esta sección, se describe cómo instalar Kaspersky Security Center Linux en el sistema operativo Astra Linux Special Edition.

Antes de la instalación:

- [Instale el DBMS.](#)
- Asegúrese de que el dispositivo donde desea instalar Kaspersky Security Center Linux esté ejecutando una de las [distribuciones de Linux compatibles](#).
- Descargue la clave de la [aplicación kaspersky_astra_pub_key.gpg](#).

Utilice el archivo de instalación ksc64_[número_de_versión]_amd64.deb. El archivo de instalación debe descargarse del sitio web de Kaspersky.

Ejecute los comandos provistos en esta instrucción bajo una cuenta con privilegios de raíz.

Para instalar Kaspersky Security Center Linux en el sistema operativo Astra Linux Special Edition (actualización operativa 1.7.2) y Astra Linux Special Edition (actualización operativa 1.6), siga estos pasos:

1. Abra el archivo /etc/digisig/digisig_initramfs.conf y especifique el siguiente ajuste:

```
DIGSIG_ELF_MODE=1
```

2. En la línea de comandos, ejecute el siguiente comando para instalar el paquete de compatibilidad:

```
apt install astra-digisig-oldkeys
```

3. Cree un directorio para la clave de la aplicación:

```
mkdir -p /etc/digisig/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/digisig/keys/legacy/kaspersky/
```

5. Actualice los discos RAM:

```
update-initramfs -u -k all
```

Reinicie el sistema.

6. Cree un grupo 'kladmins' y una cuenta sin privilegios 'ksc'. La cuenta debe ser miembro del grupo 'kladmins'. Para hacer esto, ejecute los siguientes comandos en secuencia:

```
# adduser ksc
# groupadd kladmins
# gpasswd -a ksc kladmins
# usermod -g kladmins ksc
```

7. Ejecute la instalación de Kaspersky Security Center Linux:

```
# apt install /<path>/ksc64_[version_number]_amd64.deb
```

8. Ejecute la configuración de Kaspersky Security Center Linux:

```
# /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

9. Lea el [Contrato de licencia de usuario final](#) (EULA) y la Política de privacidad. El texto se muestra en la ventana de la línea de comandos. Presione la barra espaciadora para ver el siguiente segmento de texto. Cuando se le solicite, ingrese los siguientes valores:

a. Ingrese `y` si entiende y acepta los términos del EULA. Ingrese `n` si no acepta los términos del EULA. Para usar Kaspersky Security Center Linux, debe aceptar las condiciones del EULA.

b. Ingrese `y` si comprende y acepta los términos de la Política de privacidad, y acepta que sus datos se manejarán y transmitirán (incluso a terceros países) como se describe en la Política de privacidad. Ingrese `n`

si no acepta los términos de la Política de privacidad. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos de la Política de privacidad.

10. Cuando se lo solicite, ingrese los siguientes ajustes:

- a. Ingrese el nombre DNS o la dirección IP estática del Servidor de administración.
- b. Introduzca el número de puerto del Servidor de administración. De manera predeterminada, se utiliza el puerto 14000.
- c. Introduzca el número de puerto SSL del Servidor de administración. De manera predeterminada, se utiliza el puerto 13000.
- d. Evalúe el número aproximado de dispositivos que desea administrar:
 - Si tiene de 1 a 100 dispositivos en red, ingrese 1.
 - Si tiene de 101 a 1000 dispositivos en red, ingrese 2.
 - Si tiene más de 1000 dispositivos en red, ingrese 3.
- e. Ingrese el nombre del grupo de seguridad para los servicios. De forma predeterminada, se utiliza el grupo 'kladmins'.
- f. Introduzca el nombre de la cuenta para iniciar el servicio del Servidor de administración. La cuenta debe ser miembro del grupo de seguridad ingresado. De forma predeterminada, se utiliza la cuenta 'ksc'.
- g. Introduzca el nombre de la cuenta para iniciar otros servicios. La cuenta debe ser miembro del grupo de seguridad ingresado. De forma predeterminada, se utiliza la cuenta 'ksc'.
- h. Introduzca la dirección IP del dispositivo en el que está instalada la base de datos.
- i. Introduzca el número de puerto de la base de datos. Este puerto se utiliza para comunicarse con el Servidor de administración. De manera predeterminada, se utiliza el puerto 3306.
- j. Introduzca el nombre de la base de datos.
- k. Introduzca el inicio de sesión de la cuenta root de la base de datos que utiliza para acceder a la base de datos.
- l. Introduzca la contraseña de la cuenta root de la base de datos que utiliza para acceder a la base de datos. Espere a que los servicios se añadan e inicien automáticamente:
 - klnagent_srv
 - kladminserver_srv
 - klactprx_srv
 - klwebsrv_srv
- m. Cree una cuenta que actuará como administrador del Servidor de administración. Introduzca el nombre de usuario y la contraseña.

La contraseña debe cumplir con las siguientes reglas:

 - La contraseña de usuario debe tener un mínimo de 8 y un máximo de 16 caracteres.

- La contraseña debe contener caracteres de al menos tres de los grupos enumerados a continuación:
 - Letras mayúsculas (A-Z)
 - Letras minúsculas (a-z)
 - Números (0-9)
 - Caracteres especiales (@ # \$ % ^ & * - _ ! + = [] { } | : ' . ? / \ ` ~ " () ;)

Se instala Kaspersky Security Center Linux y se añade el usuario.

Verificación del servicio

Use los siguientes comandos para verificar si un servicio se está ejecutando o no:

- # `systemctl status klnagent_srv.service`
- # `systemctl status kladminserver_srv.service`
- # `systemctl status klactprx_srv.service`
- # `systemctl status klwebsrv_srv.service`

Instalación de Kaspersky Security Center Web Console

En esta sección, se describe cómo instalar el Servidor de Kaspersky Security Center Web Console (en lo sucesivo, también se usará la denominación "Kaspersky Security Center Web Console") en dispositivos con el sistema operativo Linux. Antes de la instalación, debe [instalar un DBMS](#) y el Servidor de administración de [Kaspersky Security Center Linux](#).

Si instala Kaspersky Security Center Web Console en Astra Linux en el modo de entorno de software cerrado, siga las [instrucciones específicas para Astra Linux](#).

Utilice uno de los siguientes archivos de instalación que corresponda a la distribución de Linux instalada en su dispositivo:

- Para Debian: `ksc-web-console-[número_de_compilación].x86_64.deb`
- Para sistemas operativos basados en RPM: `ksc-web-console-[número_de_compilación].x86_64.rpm`
- Para ALT 8 SP: `ksc-web-console-[build_number]-alt8p.x86_64.rpm`

El archivo de instalación debe descargarse del sitio web de Kaspersky.

Para instalar Kaspersky Security Center Web Console:

1. Asegúrese de que el dispositivo en el que desea instalar Kaspersky Security Center Web Console esté ejecutando una de las distribuciones de Linux compatibles.

2. Lea el Contrato de licencia de usuario final (EULA, por las siglas del término en inglés). Si el kit de distribución de Kaspersky Security Center Linux no incluye un archivo TXT con el texto del EULA, puede descargar el archivo desde el [sitio web de Kaspersky](#). Si no acepta los términos del Contrato de licencia, no instale la aplicación.
3. Cree un [archivo de respuesta](#) que contenga parámetros para conectar Kaspersky Security Center Web Console al Servidor de administración. Nombre a este archivo ksc-web-console-setup.json y colóquelo en el siguiente directorio: /etc/ksc-web-console-setup.json.

Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros, y la dirección y el puerto predeterminados:

```
{
  "address": "127.0.0.1",
  "port": 8080,
  "trusted":
  "127.0.0.1|13299|/var/opt/kaspersky/klInagent_srv/1093/cert/klserver.cer|KSC
  Server",
  "acceptEula": true
}
```

Cuando instala Kaspersky Security Center Web Console en el sistema operativo Linux ALT, debe especificar un número de puerto que no sea 8080, ya que el sistema operativo usa el puerto 8080.

Kaspersky Security Center Web Console no se puede actualizar con el archivo .rpm utilizado para la instalación. Si desea cambiar la configuración de un archivo de respuestas y usar este archivo para reinstalar la aplicación, primero debe eliminar la aplicación y luego volver a instalarla con el nuevo archivo de respuestas.

4. Con una cuenta con privilegios root, use la línea de comandos para ejecutar el archivo de instalación con la extensión .deb o .rpm, dependiendo de su distribución de Linux.
 - Para instalar o actualizar Kaspersky Security Center Web Console con un archivo .deb, ejecute el siguiente comando:

```
$ sudo dpkg -i ksc-web-console-[ número_de_compilación ].x86_64.deb
```
 - Para instalar Kaspersky Security Center Web Console desde un archivo .rpm, ejecute uno de los siguientes comandos:

```
$ sudo rpm -ivh --nodeps ksc-web-console-[ número_de_compilación ].x86_64.rpm
```

o

```
$ sudo alien -i ksc-web-console-[ número_de_compilación ].x86_64.rpm
```
 - Para actualizar Kaspersky Security Center Web Console a una versión más reciente, ejecute uno de estos comandos:
 - Para dispositivos que ejecutan un sistema operativo basado en RPM:

```
$ sudo rpm -Uvh --nodeps --force ksc-web-console-[ número_de_compilación ].x86_64.rpm
```
 - Para dispositivos que ejecutan un sistema operativo basado en Debian:

```
$ sudo dpkg -i ksc-web-console-[ número_de_compilación ].x86_64.deb
```

Se iniciará el proceso para desempaquetar el archivo de instalación. Espere a que se complete la instalación. Kaspersky Security Center Web Console se instala en el siguiente directorio: /var/opt/kaspersky/ksc-web-console.

5. Ejecute el siguiente comando para reiniciar todos los servicios de Kaspersky Security Center Web Console:
- ```
$ sudo systemctl restart KSC*
```

Cuando finalice la instalación, puede usar su navegador para [abrir e iniciar sesión en Kaspersky Security Center Web Console](#).

## Parámetros de instalación de Kaspersky Security Center Web Console

Para [instalar el servidor Kaspersky Security Center Web Console en dispositivos que ejecutan Linux](#), debe crear un archivo de respuesta: un archivo .json que contenga parámetros para conectar Kaspersky Security Center Web Console al Servidor de administración.

Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros, y la dirección y el puerto predeterminados:

```
{
 "address": "127.0.0.1",
 "port": 8080,
 "defaultLangId": 1049,
 "enableLog": false,
 "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
 "acceptEula": true,
 "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
 "webConsoleAccount": "Grupo1 : Usuario1",
 "managementServiceAccount": "Grupo1 : Usuario2",
 "serviceWebConsoleAccount": "Grupo1 : Usuario3",
 "pluginAccount": "Grupo1 : Usuario4",
 "messageQueueAccount": "Grupo1 : Usuario5"
}
```

Cuando instale Kaspersky Security Center Web Console en el sistema operativo Linux ALT, debe especificar un número de puerto distinto del 8080, debido a que el sistema operativo utiliza el puerto 8080.

En la siguiente tabla se describen los parámetros que se pueden especificar en un archivo de respuesta.

Parámetros para instalar Kaspersky Security Center Web Console en dispositivos que ejecutan Linux

| Parámetro     | Descripción                                                                                                                                    | Valores disponi                                                                                               |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| address       | Dirección del Servidor de Kaspersky Security Center Web Console (obligatorio).                                                                 | Valor de cadena.                                                                                              |
| puerto        | Número de puerto que utiliza el Servidor de Kaspersky Security Center Web Console para conectarse al Servidor de administración (obligatorio). | Valor numérico.                                                                                               |
| defaultLangId | Idioma de la interfaz de usuario (de forma predeterminada, 1033).                                                                              | Código numérico del idioma: <ul style="list-style-type: none"><li>Alemán: 1031</li><li>Inglés: 1033</li></ul> |

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• Español: 3082</li> <li>• Español (México): 2058</li> <li>• Francés: 1036</li> <li>• Japonés: 1041</li> <li>• Kazajo: 1087</li> <li>• Polaco: 1045</li> <li>• Portugués (Brasil): 1046</li> <li>• Ruso: 1049</li> <li>• Turco: 1055</li> <li>• Chino simplificado: 4</li> <li>• Chino tradicional: 31748</li> </ul> <p>Si no se especifica ningún valor, se usa el</p> |
| <b>enableLog</b> | Activar o no activar el registro de actividad de Kaspersky Security Center Web Console                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>Valor booleano:</p> <ul style="list-style-type: none"> <li>• true: el registro está habilitado (selec predeterminada).</li> <li>• false: el registro está desactivado.</li> </ul>                                                                                                                                                                                                                           |
| <b>trusted</b>   | <p>Lista de servidores de administración de confianza con derecho a conectarse a Kaspersky Security Center Web Console. Cada Servidor de administración se debe definir con los siguientes parámetros:</p> <ul style="list-style-type: none"> <li>• Dirección del Servidor de administración</li> <li>• El puerto de OpenAPI que utiliza Kaspersky Security Center Web Console para conectar al Servidor de administración (de forma predeterminada, 13299)</li> <li>• Ruta al certificado del Servidor de administración</li> <li>• El nombre del Servidor de administración que se mostrará en la ventana del inicio de sesión</li> </ul> | <p>Valor de cadena en el siguiente formato:</p> <p>"dirección del servidor   puerto certificado   nombre del servidor</p> <p>Ejemplo:</p> <p>"X.X.X.X 13299 /cert/servidor-1.1 Y.Y.Y.Y 13299 /cert/servidor-</p>                                                                                                                                                                                               |

|                          |                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | Los parámetros se separan con barras verticales. Si se especifican varios Servidores de administración, sepárelos con dos barras verticales.                                                                     |                                                                                                                                                                                                                                                                                                                                                         |
| acceptEula               | Aceptar o no aceptar los términos y condiciones del <a href="#">Contrato de licencia de usuario final</a> (EULA). El archivo que contiene los términos del EULA se descarga junto con el archivo de instalación. | <p>Valor booleano:</p> <ul style="list-style-type: none"> <li>• true: He leído, entendido y acepto cc del <a href="#">Contrato de licencia de usuario fir</a></li> <li>• false: No acepto los términos del Cc predeterminada).</li> </ul> <p>Si no se especifica ningún valor, el instala- Center Web Console muestra el EULA y términos del mismo.</p> |
| certDomain               | Si desea generar un nuevo certificado, use este parámetro para especificar el nombre de dominio para el que se generará un nuevo certificado.                                                                    | Valor de cadena.                                                                                                                                                                                                                                                                                                                                        |
| certPath                 | Si desea usar un certificado existente, use este parámetro para especificar la ruta al archivo de clave.                                                                                                         | <p>Valor de cadena.</p> <p>Especifique la ruta "/var/opt/kaspersky/klnagent_srv para utilizar el certificado existente. Para especifique la ruta donde se almacena es</p>                                                                                                                                                                               |
| keyPath                  | Si desea usar un certificado existente, use este parámetro para especificar la ruta al archivo de certificado.                                                                                                   | Valor de cadena.                                                                                                                                                                                                                                                                                                                                        |
| webConsoleAccount        | Nombre de la cuenta con la cual se está ejecutando el servicio <a href="#">KSCWebConsole</a> .                                                                                                                   | <p>Valor de cadena con el siguiente formato grupo : nombre de usuario " .</p> <p>Ejemplo: " Grupo1 : Usuario1 " .</p> <p>Si no se especifica ningún valor, el instala- Center Web Console crea una nueva cue predeterminado user_management_%ui</p>                                                                                                     |
| managementServiceAccount | Nombre de la cuenta privilegiada bajo la cual se ejecuta el servicio <a href="#">KSCWebConsoleManagement</a> .                                                                                                   | <p>Valor de cadena con el siguiente formato grupo : nombre de usuario " .</p> <p>Ejemplo: " Grupo1 : Usuario1 " .</p> <p>Si no se especifica ningún valor, el instala- Center Web Console crea una nueva cue predeterminado user_nodejs_%uid%.</p>                                                                                                      |
| serviceWebConsoleAccount | Nombre de la cuenta privilegiada bajo la cual se ejecuta el servicio <a href="#">KSCSvcWebConsole</a> .                                                                                                          | <p>Valor de cadena con el siguiente formato grupo : nombre de usuario " .</p> <p>Ejemplo: " Grupo1 : Usuario1 " .</p> <p>Si no se especifica ningún valor, el instala- Center Web Console crea una nueva cue predeterminado user_svc_nodejs_%ui</p>                                                                                                     |
| pluginAccount            | Nombre de la cuenta con la cual se está ejecutando el servicio <a href="#">KSCWebConsolePlugin</a> .                                                                                                             | <p>Valor de cadena con el siguiente formato grupo : nombre de usuario " .</p> <p>Ejemplo: " Grupo1 : Usuario1 " .</p>                                                                                                                                                                                                                                   |

|                                  |                                                                                                            |                                                                                                                                                                                                                                                                                     |
|----------------------------------|------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                  |                                                                                                            | Si no se especifica ningún valor, el instalador de Center Web Console crea una nueva cuenta predeterminada <code>user_web_plugin_%ui</code> .                                                                                                                                       |
| <code>messageQueueAccount</code> | Nombre de la cuenta con la cual se está ejecutando el servicio <a href="#">KSCWebConsoleMessageQueue</a> . | Valor de cadena con el siguiente formato <code>grupo : nombre de usuario</code> .<br>Ejemplo: <code>" Grupo1 : Usuario1 "</code> .<br>Si no se especifica ningún valor, el instalador de Center Web Console crea una nueva cuenta predeterminada <code>user_message_queue_</code> . |

Si especifica los parámetros `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` o `messageQueueAccount`, asegúrese de que las cuentas de usuario personalizadas pertenezcan al mismo grupo de seguridad. Si no se especifican estos parámetros, el instalador de Kaspersky Security Center Web Console creará un grupo de seguridad predeterminado y luego creará cuentas de usuario con nombres predeterminados en el grupo.

## Instalación de Kaspersky Security Center Web Console en Astra Linux en el modo de entorno de software cerrado

En esta sección, se describe cómo instalar el Servidor de Kaspersky Security Center Web Console (en lo sucesivo, también se usará la denominación "Kaspersky Security Center Web Console") en el sistema operativo Astra Linux Special Edition. Antes de la instalación, debe [instalar un DBMS](#) y el Servidor de administración de [Kaspersky Security Center Linux](#).

*Para instalar Kaspersky Security Center Web Console:*

1. Asegúrese de que el dispositivo en el que desea instalar Kaspersky Security Center Web Console esté ejecutando una de las distribuciones de Linux compatibles.
2. Lea el Contrato de licencia de usuario final (EULA, por las siglas del término en inglés). Si el kit de distribución de Kaspersky Security Center Linux no incluye un archivo TXT con el texto del EULA, puede descargar el archivo desde el [sitio web de Kaspersky](#). Si no acepta los términos del Contrato de licencia, no instale la aplicación.
3. Cree un [archivo de respuesta](#) que contenga parámetros para conectar Kaspersky Security Center Web Console al Servidor de administración. Nombre a este archivo `ksc-web-console-setup.json` y colóquelo en el siguiente directorio: `/etc/ksc-web-console-setup.json`.

Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros, y la dirección y el puerto predeterminados:

```
{
 "address": "127.0.0.1",
 "port": 8080,
 "trusted":
 "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
 Server",
 "acceptEula": true
}
```

4. Abra el archivo `/etc/digsig/digsig_initramfs.conf` y especifique el siguiente ajuste:

```
DIGSIG_ELF_MODE=1
```

5. En la línea de comandos, ejecute el siguiente comando para instalar el paquete de compatibilidad:

```
apt install astra-digsig-oldkeys
```

6. Cree un directorio para la clave de la aplicación:

```
mkdir -p /etc/digsig/keys/legacy/kaspersky/
```

7. Coloque la clave de la aplicación /opt/kaspersky/ksc64/share/kaspersky\_astra\_pub\_key.gpg 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 Linux no incluye la clave de la aplicación kaspersky\_astra\_pub\_key.gpg, puede descargarla haciendo clic en el enlace:

[https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky\\_astra\\_pub\\_key.gpg](https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg).

8. Actualice los discos RAM:

```
update-initramfs -u -k all
```

Reinicie el sistema.

9. En una cuenta con privilegios de raíz, utilice la línea de comandos para ejecutar el archivo de instalación. El archivo de instalación debe descargarse del sitio web de Kaspersky.

- Para instalar o actualizar Kaspersky Security Center Web Console, ejecute el siguiente comando:  
\$ sudo dpkg -i ksc-web-console-[ número\_de\_compilación ].x86\_64.deb
- Para actualizar Kaspersky Security Center Web Console a una versión más reciente, ejecute el siguiente comando:  
\$ sudo dpkg -i ksc-web-console-[ número\_de\_compilación ].x86\_64.deb

Se iniciará el proceso para desempaquetar el archivo de instalación. Espere a que se complete la instalación. Kaspersky Security Center Web Console se instala en el siguiente directorio: /var/opt/kaspersky/ksc-web-console.

10. Ejecute el siguiente comando para reiniciar todos los servicios de Kaspersky Security Center Web Console:

```
$ sudo systemctl restart KSC*
```

Cuando finalice la instalación, puede usar su navegador para [abrir e iniciar sesión en Kaspersky Security Center Web Console](#).

## Instalación de Kaspersky Security Center Web Console conectado al Servidor de administración instalado en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux

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 Linux. Antes de instalar Kaspersky Security Center Web Console, [instale un DBMS](#) y el Servidor de administración de Kaspersky Security Center Linux en los [nodos del clúster de conmutación por error de Kaspersky Security Center Linux](#).

*Para instalar 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 Linux, siga estos pasos:*



1. Siga los pasos 1 y 2 de la [Instalación de Kaspersky Security Center Web Console](#).

2. En el paso 3, en el [archivo de respuesta](#), especifique el parámetro de instalación `trusted` para permitir que el clúster de conmutación por error de Kaspersky Security Center Linux se conecte a Kaspersky Security Center Web Console. El valor de cadena de este parámetro tiene el siguiente formato:

```
"trusted": "server address|port|certificate path|server name"
```

Especifique los componentes del parámetro de instalación `trusted`:

- **Dirección de Servidor de administración.** Si ha creado un adaptador de red secundario al [preparar los nodos del clúster](#), use la dirección IP del adaptador como la dirección del clúster de conmutación por error de Kaspersky Security Center Linux. De lo contrario, ingrese la dirección IP del equilibrador de carga de terceros que esté utilizando.
- **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 compartido del [clúster de conmutación por error de Kaspersky Security Center Linux](#). 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.
- **Nombre del Servidor de administración.** Es el nombre del clúster de conmutación por error de Kaspersky Security Center Linux que se mostrará en la ventana de inicio de sesión de Kaspersky Security Center Web Console.

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.

Puede ir a **Detección y despliegue** → **Dispositivos no asignados** para ver la información sobre los nodos del clúster y el [servidor de archivos](#).

## Despliegue del clúster de conmutación por error de Kaspersky Security Center Linux

Esta sección contiene información general sobre el clúster de conmutación por error de Kaspersky Security Center Linux e instrucciones sobre la preparación y el despliegue del clúster de conmutación por error de Kaspersky Security Center Linux en su red.

## Escenario: Despliegue del clúster de conmutación por error de Kaspersky Security Center Linux

Un clúster de conmutación por error de Kaspersky Security Center Linux proporciona una alta disponibilidad de Kaspersky Security Center Linux y minimiza el tiempo de inactividad del Servidor de administración en caso de un fallo. El clúster de conmutación por error se basa en dos instancias idénticas de Kaspersky Security Center Linux 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

Dispone de hardware que cumple los [requisitos](#) del clúster de conmutación por error.

El despliegue de las aplicaciones de Kaspersky se divide en etapas:

### 1 Creación de cuentas para los servicios de Kaspersky Security Center Linux

Siga estos pasos en el nodo activo, el nodo pasivo y el servidor de archivos:

1. Cree un grupo de dominio con el nombre "kladmins" y asigne el mismo GID a los tres grupos.
2. Cree una cuenta de usuario con el nombre "ksc" y asigne el mismo UID a las tres cuentas de usuario. Defina el grupo principal como 'kladmins' para las cuentas creadas.
3. Cree una cuenta de usuario con el nombre "rightless" y asigne el mismo UID a las tres cuentas de usuario. Defina el grupo principal como 'kladmins' para las cuentas creadas.

### 2 Preparación del servidor de archivos

Prepare el servidor de archivos para que funcione como componente del clúster de conmutación por error de Kaspersky Security Center Linux. Asegúrese de que el servidor de archivos cumple los requisitos de hardware y software, cree dos carpetas compartidas para los datos de Kaspersky Security Center Linux 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 Linux](#)

### 3 Preparación de nodos activos y pasivos

Prepare dos equipos con hardware y software idénticos para que funcionen como un nodo activo y pasivo.

Instrucciones: [Preparación de nodos para el clúster de conmutación por error de Kaspersky Security Center Linux](#)

### 4 Instalación del sistema de administración de bases de datos (DBMS)

Usted cuenta con dos opciones:

- Si desea utilizar MariaDB Galera Cluster, no necesita un ordenador dedicado para la DBMS. Instale MariaDB Galera Cluster en cada uno de los nodos.
- Si desea utilizar cualquier otro [DBMS compatible](#), [instale](#) el DBMS elegido en un equipo dedicado.

### 5 Instalación de Kaspersky Security Center Linux

Instale Kaspersky Security Center Linux en el modo de clúster de conmutación por error en ambos nodos. Primero debe instalar Kaspersky Security Center Linux en el nodo activo y luego, en el pasivo.

Además, puede [instalar Kaspersky Security Center Web Console](#) en un dispositivo independiente que no sea un nodo del clúster.

### 6 Prueba del clúster de conmutación por error

Compruebe que ha configurado correctamente el clúster de conmutación por error y que funciona como debe. Por ejemplo, puede detener uno de los servicios de Kaspersky Security Center Linux en el nodo activo: kladminserver, klnagent, ksnproxy, klactprx o klwebsrv. Una vez detenido el servicio, la administración de la protección debe pasar automáticamente al nodo pasivo.

## Resultados

El clúster de conmutación por error de Kaspersky Security Center Linux está 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 Linux

Un clúster de conmutación por error de Kaspersky Security Center Linux proporciona una alta disponibilidad de Kaspersky Security Center Linux y minimiza el tiempo de inactividad del Servidor de administración en caso de un fallo. El clúster de conmutación por error se basa en dos instancias idénticas de Kaspersky Security Center Linux 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.

En un clúster de conmutación por error de Kaspersky Security Center Linux, todos los servicios de Kaspersky Security Center Linux se administran de forma automática. No intente reiniciar los servicios manualmente.

### Requisitos de hardware y software

Para desplegar un clúster de conmutación por error de Kaspersky Security Center Linux, debe tener el siguiente hardware:

- Dos equipos con idéntico hardware y software. Estos equipos actuarán como nodos activos y pasivos.
- Un servidor de archivos que ejecuta Linux, con el sistema de archivos EXT4. Debe proporcionar un equipo dedicado que actuará como servidor de archivos.

Asegúrese de haber proporcionado un ancho de banda de red elevado entre el servidor de archivos y los nodos activo y pasivo.

- Un equipo con sistema de administración de base de datos (DBMS). Si usa MariaDB Galera Cluster como un DBMS, no se requiere un ordenador dedicado para este propósito.

### Condiciones para el cambio

El clúster de conmutación por error cambia la administración de la protección de los dispositivos cliente del nodo activo al nodo pasivo si se produce 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 detuvo temporalmente por actividades de [mantenimiento](#).
- Al menos uno de los servicios (o procesos) de Kaspersky Security Center Linux falló o fue cancelado deliberadamente por el usuario. Los servicios de Kaspersky Security Center Linux 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.

# Preparación de un servidor de archivos para un clúster de conmutación por error de Kaspersky Security Center Linux

Un servidor de archivos funciona como un componente necesario de un [clúster de conmutación por error de Kaspersky Security Center Linux](#).

Para preparar un servidor de archivos, haga lo siguiente:

1. Asegúrese de que el servidor de archivos cumpla los [requisitos de hardware y software](#).
2. Instale y configure un servidor NFS:
  - El acceso al servidor de archivos debe estar habilitado para ambos nodos en la configuración del servidor NFS.
  - El protocolo NFS debe tener la versión 4.0 o 4.1.
  - Requisitos mínimos para el núcleo de Linux:
    - 3.19.0-25 si usa NFS 4.0
    - 4.4.0-176, si usa NFS 4.1
3. En el servidor de archivos, cree dos carpetas y compártalas mediante NFS. 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 Linux. Usted especificará las rutas a las carpetas compartidas mientras configura la [instalación de Kaspersky Security Center Linux](#).

Ejecute los siguientes comandos:

```
sudo yum instalar nfs-utils
sudo mkdir -p /mnt/KlFocStateShare
sudo mkdir -p /mnt/KlFocDataShare_klfoc
sudo chown ksc:kladmins /mnt/KlFocStateShare
sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
sudo chmod -R 777 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
sudo sh -c "echo /mnt/KlFocStateShare *(rw, sync, no_subtree_check, no_root_squash) >> /etc/exports"
sudo sh -c "echo /mnt/KlFocDataShare_klfoc *(rw, sync, no_subtree_check, no_root_squash) >> /etc/exports"
sudo cat /etc/exports
sudo exportfs -a
sudo systemctl start rpcbind
sudo service nfs start
```

Active el inicio automático ejecutando el siguiente comando:

```
sudo systemctl enable rpcbind
```

4. Reinicie el servidor de archivos.

El servidor de archivos está preparado. Para desplegar el clúster de conmutación por error de Kaspersky Security Center Linux, siga las instrucciones de este [escenario](#).

# Preparación de nodos para un clúster de conmutación por error de Kaspersky Security Center Linux

Prepare dos equipos para que funcionen como nodos activo y pasivo del [clúster de conmutación por error de Kaspersky Security Center Linux](#).

Para preparar los nodos del clúster de conmutación por error de Kaspersky Security Center Linux, haga lo siguiente:

1. Asegúrese de que tenga dos equipos que cumplen los [requisitos de hardware y software](#). Estos equipos actuarán como nodos activos y pasivos del clúster de conmutación por error.

2. Para que los nodos funcionen como clientes NFS, instale el paquete `nfs-utils` en cada nodo.

Ejecute el siguiente comando:

```
sudo yum instalar nfs-utils
```

3. Cree puntos de montaje con los siguientes comandos:

```
sudo mkdir -p /mnt/KlFocStateShare
sudo mkdir -p /mnt/KlFocDataShare_klfoc
```

4. Compruebe que las carpetas compartidas se puedan montar correctamente. [paso opcional]

Ejecute los siguientes comandos:

```
sudo mount -t nfs -o vers=4,noexec,local_lock=none,auto,user,rw {server}:{ruta a la
carpeta KlFocStateShare} /mnt/KlFocStateShare
sudo mount -t nfs -o vers=4,noexec,local_lock=none,noauto,user,rw {server}:{ruta a
la carpeta KlFocDataShare_klfoc} /mnt/KlFocDataShare_klfoc
```

Aquí, `{server}:{ruta a la carpeta KlFocStateShare}` y `{server}:{ruta a la carpeta KlFocDataShare_klfoc}` son las rutas de red a las carpetas compartidas en el servidor de archivos.

Una vez que las carpetas compartidas se hayan montado correctamente, desmóntelas ejecutando los siguientes comandos:

```
sudo umount /mnt/KlFocStateShare
sudo umount /mnt/KlFocDataShare_klfoc
```

5. Haga coincidir los puntos de montaje y las carpetas compartidas:

```
sudo vi /etc/fstab
{server}:{ruta a la carpeta KlFocStateShare} /mnt/KlFocStateShare nfs
vers=4,noexec,local_lock=none,auto,user,rw 0 0
{server}:{ruta a la carpeta KlFocDataShare_klfoc} /mnt/KlFocDataShare_klfoc nfs
vers=4,noexec,local_lock=none,noauto,user,rw 0 0
```

Aquí, `{server}:{ruta a la carpeta KlFocStateShare}` y `{server}:{ruta a la carpeta KlFocDataShare_klfoc}` son las rutas de red a las carpetas compartidas en el servidor de archivos.

6. Reinicie ambos nodos.

7. Monte las carpetas compartidas ejecutando los siguientes comandos:

```
mount /mnt/KlFocStateShare
mount /mnt/KlFocDataShare_klfoc
```

8. Asegúrese de que los permisos para acceder a las carpetas compartidas pertenezcan a `ksc:kladmins`.

Ejecute el siguiente comando:

```
sudo ls -la /mnt/
```

## 9. 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.

Realice una de las siguientes acciones:

- Utilice un adaptador de red virtual.
  - a. Utilice el siguiente comando para verificar que NetworkManager se usa para administrar el adaptador físico:  

```
nmcli device status
```

Si el adaptador físico aparece como no administrado en la salida, configure NetworkManager para administrar el adaptador físico. Los pasos de configuración exactos dependen de su distribución.
  - b. Utilice el siguiente comando para identificar las interfaces:  

```
ip a
```
  - c. Cree un nuevo perfil de configuración:  

```
nmcli connection add type macvlan dev <interfaz física> mode bridge ifname <interfaz virtual> ipv4.addresses <máscara de dirección> ipv4.method manual autoconnect no
```
- Utilice un adaptador de red físico o un hipervisor. En este escenario, desactive el software NetworkManager.
  - a. Elimine las conexiones de NetworkManager para la interfaz de destino:  

```
nmcli con del <nombre de conexión>
```

Use el siguiente comando para comprobar si la interfaz de destino tiene conexiones:  

```
nmcli con show
```
  - b. Edite el archivo NetworkManager.conf. Busque la sección del archivo clave y asigne la interfaz de destino al parámetro unmanaged-devices.  

```
[keyfile]
unmanaged-devices=interface-name:<nombre de interfaz>
```
  - c. Reinicie NetworkManager:  

```
systemctl reload NetworkManager
```

Use el siguiente comando para comprobar que la interfaz de destino no esté administrada:  

```
nmcli dev status
```
- Utilice un equilibrador de carga de terceros. Por ejemplo, puede utilizar un servidor nginx. En este caso, haga lo siguiente:
  - a. Proporcione un equipo dedicado basado en Linux con nginx instalado.
  - b. Configure el equilibrio de carga. Establezca el nodo activo como servidor principal y el nodo pasivo como servidor de reserva.
  - c. En el servidor nginx, abra todos los puertos del Servidor de administración: TCP 13000, UDP 13000, TCP 13291, TCP 13299 y TCP 17000.

Los nodos están preparados. Para desplegar el clúster de conmutación por error de Kaspersky Security Center Linux, siga las demás instrucciones del [escenario](#).

# Instalación de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux

En este procedimiento, se describe cómo instalar Kaspersky Security Center Linux en los nodos del [clúster de conmutación por error de Kaspersky Security Center Linux](#). Kaspersky Security Center Linux se instala por separado en ambos nodos del clúster de conmutación por error de Kaspersky Security Center Linux. 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.

Utilice el archivo de instalación — `ksc64_[version_number]_amd64.deb` o `ksc64-[version_number].x86_64.rpm` — que corresponda a la distribución de Linux instalada en su dispositivo. El archivo de instalación debe descargarse del sitio web de Kaspersky.

Solo un usuario del grupo de dominio KAdmins puede instalar Kaspersky Security Center Linux en cada nodo.

## Instalación en el nodo principal (activo)

*Para instalar Kaspersky Security Center Linux en el nodo principal:*

1. Asegúrese de que el dispositivo donde desea instalar Kaspersky Security Center Linux esté ejecutando una de las [distribuciones de Linux compatibles](#).
2. En la línea de comandos, ejecute los comandos provistos en esta instrucción bajo una cuenta con privilegios de raíz.
3. Ejecute la instalación de Kaspersky Security Center Linux. Según su distribución de Linux, ejecute uno de los siguientes comandos:
  - `sudo apt install /<path>/ksc64_[version_number]_amd64.deb`
  - `sudo yum install /<path>/ksc64-[version_number].x86_64.rpm -y`
4. Ejecute la configuración de Kaspersky Security Center Linux:

```
sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```
5. Lea el [Contrato de licencia de usuario final](#) (EULA) y la Política de privacidad. 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 lo solicite, ingrese los siguientes valores:
  - a. Ingrese `y` si entiende y acepta los términos del EULA. Ingrese `n` si no acepta los términos del EULA. Para usar Kaspersky Security Center Linux, debe aceptar las condiciones del EULA.
  - b. Ingrese `y` si comprende y acepta los términos de la Política de privacidad, y acepta que sus datos se manejarán y transmitirán (incluso a terceros países) como se describe en la Política de privacidad. Ingrese `n` si no acepta los términos de la Política de privacidad. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos de la Política de privacidad.
6. Seleccione **Nodo de clúster principal** como modo de instalación del Servidor de administración.
7. Cuando se lo solicite, ingrese los siguientes ajustes:

- a. Ingrese la ruta local al punto de montaje de la carpeta compartida de estados del disco.
- b. Ingrese la ruta local al punto de montaje del recurso compartido de datos.
- c. Escoja un modo de conectividad del clúster de conmutación por error: a través de un adaptador de red secundario o un equilibrador de carga externo.
- d. Si usa un adaptador de red secundario, introduzca su nombre.
- e. Cuando se le solicite introducir el nombre DNS o la dirección IP estática del Servidor de administración, introduzca la dirección IP del adaptador de red secundario o la dirección IP del equilibrador de carga externo.
- f. Introduzca el número de puerto SSL del Servidor de administración. De manera predeterminada, se utiliza el puerto 13000.
- g. Evalúe el número aproximado de dispositivos que desea administrar:
- Si tiene de 1 a 100 dispositivos en red, ingrese 1.
  - Si tiene de 101 a 1000 dispositivos en red, ingrese 2.
  - Si tiene más de 1000 dispositivos en red, ingrese 3.
- h. Ingrese el nombre del grupo de seguridad para los servicios. De forma predeterminada, se utiliza el grupo 'kladmins'.
- i. Introduzca el nombre de la cuenta para iniciar el servicio del Servidor de administración. La cuenta debe ser miembro del grupo de seguridad ingresado. De forma predeterminada, se utiliza la cuenta 'ksc'.
- j. Introduzca el nombre de la cuenta para iniciar otros servicios. La cuenta debe ser miembro del grupo de seguridad ingresado. De forma predeterminada, se utiliza la cuenta 'ksc'.
- k. Seleccione el DBMS que instaló para trabajar con Kaspersky Security Center Linux:
- Si instaló MySQL o MariaDB, introduzca 1.
  - Si instaló Postgre SQL o Postgres Pro, ingrese 2.
- l. Introduzca el nombre de DNS o la dirección IP del dispositivo en el que está instalada la base de datos.
- m. Introduzca el número de puerto de la base de datos. Este puerto se utiliza para comunicarse con el Servidor de administración. De forma predeterminada, se utilizan los siguientes puertos:
- Puerto 3306 para MySQL o MariaDB
  - Puerto 5432 para PostgreSQL o Postgres Pro
- n. Introduzca el nombre de la base de datos.
- o. Introduzca el inicio de sesión de la cuenta root de la base de datos que utiliza para acceder a la base de datos.
- p. Introduzca la contraseña de la cuenta root de la base de datos que utiliza para acceder a la base de datos. Espere a que los servicios se añadan e inicien automáticamente:
- klnagent\_srv



- kladminserver\_srv
- klactprx\_srv
- klwebsrv\_srv

q. Cree una cuenta que actuará como administrador del Servidor de administración. Introduzca el nombre de usuario y la contraseña. La contraseña de usuario no puede tener menos de 8 ni más de 16 caracteres.

Se añade el usuario y se instala Kaspersky Security Center Linux en el nodo principal.

## Instalación en el nodo secundario (pasivo)

*Para instalar Kaspersky Security Center Linux en el nodo secundario:*

1. Asegúrese de que el dispositivo donde desea instalar Kaspersky Security Center Linux esté ejecutando una de las [distribuciones de Linux compatibles](#).
2. En la línea de comandos, ejecute los comandos provistos en esta instrucción bajo una cuenta con privilegios de raíz.
3. Ejecute la instalación de Kaspersky Security Center Linux. Según su distribución de Linux, ejecute uno de los siguientes comandos:

- `sudo apt install /<path>/ksc64-[ version_number ]_amd64.deb`
- `sudo yum install /<path>/ksc64-[ version_number ].x86_64.rpm -y`

4. Ejecute la configuración de Kaspersky Security Center Linux:

```
sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

5. Lea el [Contrato de licencia de usuario final](#) (EULA) y la Política de privacidad. 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 lo solicite, ingrese los siguientes valores:
  - a. Ingrese `y` si entiende y acepta los términos del EULA. Ingrese `n` si no acepta los términos del EULA. Para usar Kaspersky Security Center Linux, debe aceptar las condiciones del EULA.
  - b. Ingresar `y` si comprende y acepta los términos de la Política de privacidad, y acepta que sus datos se manejarán y transmitirán (incluso a terceros países) como se describe en la Política de privacidad. Ingresar `n` si no acepta los términos de la Política de privacidad. Para utilizar Kaspersky Security Center Linux, debe aceptar los términos de la Política de privacidad.

6. Seleccione **Nodo de clúster secundario** como modo de instalación del Servidor de administración.

7. Cuando se lo solicite, ingrese la ruta local al punto de montaje de la carpeta compartida de estados del disco.

Kaspersky Security Center Linux queda instalado en el nodo secundario.

## Verificación del servicio

Use los siguientes comandos para verificar si un servicio se está ejecutando o no:

- `systemctl status klagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`

Ahora, puede probar el clúster de conmutación por error de Kaspersky Security Center Linux para asegurarse de haberlo configurado de forma correcta y de que el clúster 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 Linux 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 `/opt/kaspersky/ksc64/sbin`.
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 con el comando `klfoc -stopcluster --stp klfoc`.
2. En el nodo que desea mantener, vaya a `/opt/kaspersky/ksc64/sbin`.
3. Abra la línea de comandos y, a continuación, separe el nodo del clúster con el comando `detach_node.sh`.
4. En el nodo activo, inicie el clúster de conmutación por error con el comando `klfoc -startcluster --stp klfoc`.
5. Realizar actividades de mantenimiento.
6. En el nodo activo, detenga el clúster de conmutación por error con el comando `klfoc -stopcluster --stp klfoc`.
7. En el nodo que mantuvo, vaya a `/opt/kaspersky/ksc64/sbin`.

8. Abra la línea de comandos y, a continuación, adjunte el nodo al clúster con el comando `attach_node.sh`.
9. En el nodo activo, inicie el clúster de conmutación por error con el comando `k1foc -startcluster --stp k1foc`.

El nodo se mantiene y se adjunta al clúster de conmutación por error.

## Cuentas para trabajar con el DBMS

Para instalar el Servidor de administración y trabajar con él, necesita una cuenta DBMS interna. Esta cuenta le permite acceder al DBMS y requiere derechos específicos. El conjunto de los derechos requeridos depende de los siguientes criterios:

- Tipo de DBMS:
  - MySQL o MariaDB
  - PostgreSQL o Postgres Pro
- 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 base de datos del Servidor) mediante el instalador del Servidor de administración (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, límitese 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.

Las siguientes tablas contienen información sobre los derechos de DBMS que debe otorgar a las cuentas antes de instalar e iniciar el Servidor de administración.

### MySQL y MariaDB

Si elige MySQL o MariaDB como DBMS, cree una cuenta interna de DBMS para acceder al DBMS y, a continuación, otorgue a esta cuenta los derechos necesarios. Tenga en cuenta que el método de creación de la base de datos no afecta el conjunto de derechos. Los derechos necesarios se enumeran a continuación:

- 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 (si su DBMS es MariaDB versión 10.5 o anterior, no necesita otorgar el privilegio EXECUTE).
- Privilegios globales para todos los esquemas: PROCESS, SUPER.

Para obtener más información sobre cómo configurar los derechos de la cuenta, consulte [Configuración de la cuenta DBMS para trabajar con 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.

### PostgreSQL o Postgres Pro

Si elige PostgreSQL o Postgres Pro como DBMS, puede usar el usuario *postgres* (función predeterminada de Postgres) o crear una nueva función de Postgres (en lo sucesivo, también denominada función) para acceder al DBMS. Según el método de creación de la base de datos del servidor, conceda los derechos necesarios a la función como se describe en la siguiente tabla. Para obtener más información sobre cómo configurar los derechos de la función, consulte [Configuración de la cuenta para trabajar con PostgreSQL o Postgres Pro](#).

Derechos de la función de Postgres

| Creación automática de bases de datos                        |                                               | Creación manual de bases de datos                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| El usuario <i>postgres</i> no requiere derechos adicionales. | Privilegios para una nueva función: CREATEDB. | Para una nueva función: <ul style="list-style-type: none"><li>• Privilegios en la base de datos del Servidor de administración: TODOS.</li><li>• Privilegios en todas las tablas del esquema público: TODOS.</li><li>• Privilegios en todas las secuencias del esquema público: TODOS.</li></ul> |

## Configuración de privilegios para recuperar los datos del Servidor de administración

Para restaurar los datos del Servidor de administración desde la copia de seguridad, la función de Postgres utilizada para acceder al DBMS debe tener los derechos de propietario en la base de datos del Servidor de administración.

## Configuración de la cuenta de DBMS para trabajar con MySQL y MariaDB

### Requisitos previos

Antes de asignar derechos a la cuenta DBMS, 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.

## Configuración de la cuenta DBMS para instalar el Servidor de administración

Para configurar la cuenta DBMS para la instalación del Servidor de Administración:

1. Utilizando 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.

Para crear una cuenta de DBMS con una contraseña, ejecute el siguiente comando:

```
/* Crear un usuario llamado KSCAdmin y especificar la contraseña para KSCAdmin */
CREATE USER '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 una cuenta de DBMS que utilice la autenticación "Contraseña nativa de MySQL", ejecute el siguiente comando:

```
CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<contraseña >';
```

- Para cambiar la autenticación de una cuenta DBMS existente, ejecute el siguiente comando:

```
ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<contraseña >';
```

3. Otorgue los siguientes privilegios la función de DBMS creada:

- 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 otorgar los privilegios necesarios a la cuenta DBMS creada, ejecute el siguiente script:

```
/* 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 ese caso, excluya el siguiente comando del script: GRANT EXECUTE ON PROCEDURE sys.table\_exists TO 'KSCAdmin'.

4. Para ver la lista de privilegios otorgados a la cuenta de DBMS, ejecute el siguiente comando:

```
SHOW grants for 'KSCAdmin';
```

5. 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 utf8
DEFAULT COLLATE utf8_general_ci;
```

Utilice el mismo nombre para la base de datos que haya especificado en el script para crear la cuenta del DBMS.

### 6. [Instale el 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.

## Configuración de la cuenta para trabajar con PostgreSQL y Postgres Pro

### Requisitos previos

Antes de asignar derechos a la cuenta DBMS, 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.

### Configuración de la cuenta DBMS para instalar el Servidor de administración (creación automática de la base de datos del Servidor de administración)

*Para configurar la cuenta DBMS para la instalación del Servidor de Administración:*

1. Ejecute un entorno para trabajar con PostgreSQL y Postgres Pro.
2. Elija una función de Postgres para acceder al DBMS. Puede seleccionar una de las siguientes funciones:
  - El usuario *postgres* (función predeterminada de Postgres).

Si usa el usuario *postgres*, no es necesario que le conceda derechos adicionales.

De forma predeterminada, el usuario de *postgres* no tiene contraseña. Sin embargo, una contraseña es necesaria para instalar Kaspersky Security Center Linux. Si desea establecer una contraseña para el usuario de *postgres*, ejecute el siguiente script:

```
ALTER USER user_name WITH PASSWORD '< contraseña >';
```

- Una nueva función de Postgres.

Si desea utilizar una nueva función de Postgres, créela y concédale el privilegio CREATEDB. Para hacer esto, ejecute el siguiente script (en este script, la función es *KSCAdmin*):

```
CREATE USER "KSCAdmin" WITH PASSWORD '< contraseña >' CREATEDB;
```

La función creada se utilizará como propietario de la base de datos del Servidor de administración (en adelante, también denominada base de datos del Servidor).

### 3. [Instale el Servidor de administración.](#)

Una vez finalizada la instalación, la base de datos del servidor se crea automáticamente y el Servidor de administración está listo para usarse.

## Configuración de la cuentas DBMS para instalar el Servidor de administración (creación manual de la base de datos del Servidor de administración)

Para configurar la cuenta DBMS para la instalación del Servidor de Administración:

1. Ejecute un entorno para trabajar con Postgres.
2. Cree una nueva función de Postgres y una base de datos del Servidor de administración. A continuación, otorgue todos los privilegios a la función en la base de datos del Servidor de administración. Para hacerlo, inicie sesión con el usuario *postgres* en la base de datos *postgres* y, a continuación, ejecute el siguiente script (en este script, la función es *KSCAdmin* y el nombre de la base de datos del Servidor de administración es *KAV*):

```
CREATE USER "KSCAdmin" WITH PASSWORD '<contraseña>';
CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
```

Si se produce el error "La nueva codificación (UTF8) no es compatible con la codificación de la base de datos de la plantilla", cree una base de datos usando el comando:

```
CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;
en lugar de:
CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
```

3. Otorgue los siguientes privilegios la función de Postgres creada:

- Privilegios en todas las tablas del esquema público: ALL
- Privilegios en todas las secuencias en el esquema público: ALL

Para hacer esto, inicie sesión con el usuario *postgres* en la base de datos del Servidor y, a continuación, ejecute el siguiente script (en este script, la función es *KSCAdmin*):

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
```

4. [Instale el 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.

## Certificados para trabajar con Kaspersky Security Center Linux

Esta sección contiene información sobre los certificados de Kaspersky Security Center Linux y describe cómo emitir y reemplazar certificados para Kaspersky Security Center Web Console y cómo renovar un certificado para el Servidor de Administración si el servidor interactúa con Kaspersky Security Center Web Console.

## 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 del Servidor web
- 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. Puede reemplazar certificados autofirmados por personalizados mediante la utilidad `klsetsrvcert` o mediante la sección de propiedades del Servidor de administración en la Kaspersky Security Center Web Console, según el tipo de certificado. 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)

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 los siguientes propósitos:

- Autenticación del Servidor de administración al conectarse a Kaspersky Security Center Web Console
- Interacción segura entre el Servidor de administración y el Agente de red en los dispositivos administrados
- Autenticación cuando los Servidores de administración primarios están conectados a los Servidores de administración secundarios

El certificado del Servidor de administración se crea automáticamente durante la instalación del componente del Servidor de administración y se guarda en la carpeta `/var/opt/kaspersky/klagent_srv/1093/cert/`. Usted especifica el certificado del Servidor de administración cuando [crea un archivo de respuesta](#) para instalar Kaspersky Security Center Web Console. El certificado del Servidor de administración se denomina certificado común ("C").

El certificado del Servidor de administración es válido por 397 días. Kaspersky Security Center genera automáticamente un certificado de reserva común ("CR") 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.

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



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. Al reemplazar el certificado, todos los Agentes de red que estaban conectados anteriormente al Servidor de administración a través de SSL perderán su conexión y devolverán el "error de autenticación del Servidor de administración". Para eliminar este error, tendrá que restaurar la conexión después del [reemplazo 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](#).

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 certificado móvil se especifica en las propiedades del Servidor de administración.

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 escenario 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"). Además, en las propiedades del Servidor de administración, puede especificar certificados cliente personalizados emitidos por una autoridad de certificación diferente, mientras que la integración con la Infraestructura de clave pública (PKI) del dominio de su organización le permite emitir certificados cliente mediante la autoridad de certificación de su dominio.

## Certificado del Servidor web

Servidor web, un componente de 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 usted descargará posteriormente en los dispositivos administrados. El Servidor web puede usar distintos certificados para tal fin.

Servidor web utiliza uno de los siguientes certificados, en orden de prioridad:

1. Certificado de servidor web personalizado que ha especificado manualmente mediante Kaspersky Security Center Web Console
2. 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 lo sucesivo, "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.

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

La siguiente tabla muestra los requisitos para los [certificados personalizados especificados para diferentes componentes de Kaspersky Security Center Linux](#).

Requisitos para los certificados de Kaspersky Security Center Linux

| Tipo de certificado                                         | Requisitos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Comentarios                                                                                                                                                                       |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certificado común, certificado de reserva común ("C", "CR") | <p>Longitud mínima de la clave: 2048.</p> <p>Restricciones básicas:</p> <ul style="list-style-type: none"> <li>• CA: cierto</li> <li>• Restricción de longitud de ruta: ninguna</li> </ul> <p>Uso de claves:</p> <ul style="list-style-type: none"> <li>• Firma digital</li> <li>• Firma de certificados</li> <li>• Cifrado de claves</li> <li>• Firma de CRL</li> </ul> <p>Uso extendido de claves (opcional): autenticación de servidor, autenticación de cliente.</p>                                                                                                      | <p>El parámetro Extended Key Usage es opcional.</p> <p>El valor de la Restricción de longitud de ruta puede ser un número entero distinto de "Ninguna", pero no inferior a 1.</p> |
| Certificado del Servidor web                                | <p>Uso extendido de clave: autenticación de servidor.</p> <p>El contenedor PKCS #12 o PEM que se utilice para especificar el certificado debe incluir toda la cadena de claves públicas.</p> <p>El campo <code>subjectAltName</code> debe tener un valor válido, es decir, debe haberse definido un nombre alternativo del sujeto (SAN) para el certificado.</p> <p>El certificado cumple con los requisitos efectivos que los navegadores web imponen a los certificados de servidor, así como con los requisitos básicos actuales del <a href="#">CA/Browser Forum</a>.</p> | N/C.                                                                                                                                                                              |
| Certificado de Kaspersky Security                           | El contenedor PEM que se utilice para especificar el certificado debe incluir toda la cadena de claves públicas.                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Kaspersky Security Center Web Console no es compatible con los certificados cifrados.                                                                                             |

|                    |                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Center Web Console | <p>El campo <code>subjectAltName</code> debe tener un valor válido, es decir, debe haberse definido un nombre alternativo del sujeto (SAN) para el certificado.</p> <p>El certificado cumple con los requisitos efectivos que los navegadores web imponen a los certificados de servidor, así como con los requisitos básicos actuales del <a href="#">CA/Browser Forum</a> <sup>2</sup>.</p> |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 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) al emitir un nuevo certificado autofirmado de forma manual. Como alternativa, puede volver a emitir su certificado de Kaspersky Security Center Web Console caducado.

Cuando abre Kaspersky Security Center Web Console, es posible que el navegador le informe de que la conexión a Kaspersky Security Center Web Console no es privada y de que el certificado de Kaspersky Security Center Web Console no es válido. Esta advertencia aparece porque el certificado de la Web Console está autofirmado y fue generado automáticamente por Kaspersky Security Center Linux. 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 Kaspersky Security Center Web Console a la lista de certificados de navegadores de confianza después de volver a emitirlo. Recomendamos que utilice esta opción solo si no puede crear un certificado personalizado.

*Para volver a emitir el certificado caducado de Kaspersky Security Center Web Console:*

Vuelva a instalar Kaspersky Security Center Web Console realizando una de las siguientes acciones:

- Si desea utilizar el mismo archivo de instalación de Kaspersky Security Center Web Console, elimine Kaspersky Security Center Web Console y luego [instale la misma versión de Kaspersky Security Center Web Console](#).
- Si desea utilizar un archivo de instalación de una versión actualizada, [ejecute el comando de actualización](#).

El certificado de Kaspersky Security Center Web Console se vuelve a emitir por otro período de validez de 397 días.

## Reemplazo del certificado de Kaspersky Security Center Web Console

De forma predeterminada, cuando instala el Servidor de Kaspersky Security Center Web Console (también conocido como Kaspersky Security Center Web Console), se genera automáticamente un certificado de navegador para la aplicación. Este certificado puede reemplazarse por uno personalizado.

*Para reemplazar el certificado de Kaspersky Security Center Web Console por uno personalizado:*

1. [Cree un nuevo archivo de respuesta](#) requerido para la instalación de Kaspersky Security Center Web Console.
2. En este archivo, especifique las rutas al archivo de certificado personalizado y al archivo de clave mediante el parámetro `certPath` y el parámetro `keyPath`.
3. Especifique el nuevo archivo de respuesta para volver a instalar Kaspersky Security Center Web Console. Realice una de las siguientes acciones:
  - Si desea utilizar el mismo archivo de instalación de Kaspersky Security Center Web Console, elimine Kaspersky Security Center Web Console y luego [instale la misma versión de Kaspersky Security Center Web Console](#).
  - Si desea utilizar un archivo de instalación de una versión actualizada, [ejecute el comando de actualización](#).

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 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 `.pen` están listos para usarse, por lo que puede especificarlos en el [instalador de Kaspersky Security Center Web Console](#).

## 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 útil reemplazar el certificado inmediatamente después de la instalación del Servidor de administración y antes de que el asistente de inicio rápido se complete.

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

## Requisitos previos

El nuevo certificado se debe crear en el formato PKCS#12 (por ejemplo, mediante la PKI de la organización) y se debe emitir a través de una autoridad de certificación (CA) de confianza. Además, el nuevo certificado debe incluir toda la cadena de confianza y una clave privada, que se debe almacenar en el archivo con la extensión pfx o p12. Para el nuevo certificado, se deben cumplir los requisitos enumerados a continuación.

Tipo de certificado: Certificado común, certificado de reserva común ("C", "CR")

Requisitos:

- Longitud mínima de la clave: 2048
- Restricciones básicas:
  - CA: cierto
  - Restricción de longitud de ruta: ninguna  
El valor de la restricción de longitud de ruta puede ser un número entero diferente de "Ninguna", pero no menos de 1.
- Uso de claves:
  - Firma digital
  - Firma de certificados
  - Cifrado de claves
  - Firma de CRL
- 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.

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

Para ello, use la línea de comandos [utilidad klsetsrvcert](#).

## 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 klmove](#).

## 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> {-i <inputfile> [-p <password>] [-o <chkopt>] | -g <dnsname>}]
[-f <time>][-r <calistfile>][-l <logfile>]
```

No necesita descargar la utilidad klsetsrvcert. Está incluida en el kit de distribución de Kaspersky Security Center Linux. No es compatible con versiones anteriores de Kaspersky Security Center Linux.

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>               | Tipo del certificado para reemplazar. Posibles valores del parámetro <tipo>: <ul style="list-style-type: none"><li>• C: Reemplace el certificado para los puertos 13000 y 13291.</li><li>• CR: Reemplace el certificado de reserva común para los puertos 13000 y 13291.</li></ul>                                                                                      |
| -f <time>               | Horario para cambiar el certificado, utilizando el formato "DD-MM-AAAA hh:mm" (para los puertos 13000 y 13291).<br>Utilice este parámetro si desea reemplazar el certificado común o 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 <archivo de entrada> | Contenedor con el certificado y una clave privada en formato PKCS#12 (archivo con extensión .p12 o .pfx).                                                                                                                                                                                                                                                               |
| -p                      | Contraseña utilizada para la protección del contenedor p12.                                                                                                                                                                                                                                                                                                             |

|                          |                                                                                                                                                                                                                                                        |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <contraseña>             | 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 <chkopt>              | Parámetros de validación del certificado (separados por punto y coma).<br>Para usar un certificado personalizado sin permiso de firma, especifique -o NoCA en la utilidad klsetsvcert. Esto es útil para los certificados emitidos por una CA pública. |
| -g <nombre dns>          | Un nuevo certificado se creará para el nombre de DNS especificado.                                                                                                                                                                                     |
| -r <calistfile>          | Lista de autoridades de certificación raíz de confianza, formato PEM.                                                                                                                                                                                  |
| -l <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:

```
klsetsvcert -t C -i <inputfile> -p <password> -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 comandos [utilidad klmove](#).

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

1. `klsetsvcert.exe -t CR -i <archivo de entrada> -p <contraseña> -o NoCA` para instalar el nuevo certificado.
2. `klsetsvcert.exe -f "DD-MM-AAAA hh:mm"` para especificar la fecha en la que se aplicará el nuevo certificado.

en el que "DD-MM-AAAA hh:mm" es la fecha 3 o 4 semanas antes de la semana actual. Modificar el momento para cambiar el antiguo certificado por el nuevo, permitirá que el nuevo certificado se distribuya a todos los agentes de red.

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

Después de reemplazar el certificado del Servidor de administración mediante la línea de comandos [utilidad klsetsvcert](#), debe establecer la conexión SSL entre los Agentes de red y el Servidor de administración porque 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:

```
klmove [-address <dirección del servidor>] [-pn <número de puerto>] [-ps <número de puerto SSL>] [-noss1] [-cert <ruta al archivo del certificado>]
```

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 activar 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 de eliminación de Kaspersky Security Center Web Console (cleaner.exe).

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 o el nombre de 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 el 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 el 13000.                  |
| -noss1                                  | 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.                                                                          |

## Definición de una carpeta compartida

Después de la instalación del Servidor de administración, puede especificar la ubicación de la carpeta compartida en las propiedades del Servidor de administración. De forma predeterminada, la carpeta compartida se crea en el dispositivo con el Servidor de administración. 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.

## Iniciar y cerrar sesión en Kaspersky Security Center Web Console



Puede iniciar sesión en Kaspersky Security Center Web Console después de [instalar el Servidor de administración y el Servidor de 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:*

1. En su navegador, vaya a <dirección web del Servidor de administración>:<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 ha añadido un único Servidor de administración, la lista de Servidores de administración está bloqueada.
3. Realice una de las siguientes acciones:

- Para iniciar sesión en el Servidor de administración con una cuenta de usuario de dominio, introduzca el nombre de usuario y la contraseña del usuario del dominio.

Puede introducir el nombre de usuario del usuario del dominio en uno de los siguientes formatos:

- nombre de usuario@dns.domain
- NTDOMAIN\nombre de usuario

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 especificando el nombre de usuario y la contraseña del administrador, introduzca el nombre de usuario y la contraseña del usuario interno.
- 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.

4. Haga clic en el botón **Iniciar 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 usarla para trabajar con Kaspersky Security Center Linux.

## Cierre de sesión

*Para cerrar sesión en Kaspersky Security Center Web Console,*

En el menú principal, vaya a la configuración de su cuenta y, a continuación, seleccione **Salir**.

Kaspersky Security Center Web Console se cierra y se muestra la página de inicio de sesión.

## 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:*

1. En el menú principal, vaya a **Configuración** → **Idioma**.
2. Seleccione uno de los idiomas admitidos.

## Configuración del servidor MySQL x64 para trabajar con Kaspersky Security Center Linux

Si utiliza el servidor MySQL para Kaspersky Security Center, habilite la compatibilidad del almacenamiento InnoDB y MEMORY, y las codificaciones UTF-8 y UCS-2.

### Configuración recomendada para el archivo my.cnf

Para obtener más detalles sobre la configuración de DBMS, consulte también el procedimiento de [configuración de la cuenta](#). Para obtener información sobre la instalación de DBMS, consulte el procedimiento de [instalación de DBMS](#).

*Para configurar el archivo my.cnf:*

1. Abra el archivo my.cnf en un editor de textos.
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
previsto 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 usar el valor del parámetro `innodb_flush_log_at_trx_commit=0`, debido a que los valores "1" o "2" afectan de modo negativo a la velocidad operativa de MySQL.

## Asistente de inicio rápido

Kaspersky Security Center Linux 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. Esta configuración se realiza mediante el asistente de inicio rápido. Cuando el asistente se está ejecutando, puede realizar 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.
- 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, así como tareas del 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 crea directivas únicamente para las aplicaciones cuya carpeta **Dispositivos administrados** no contiene directivas. El asistente de inicio rápido no crea ninguna tarea si ya existe alguna con el mismo nombre en el nivel superior de jerarquía de los dispositivos administrados.

La aplicación solicita automáticamente que se ejecute el asistente de inicio rápido tras la instalación del Servidor de administración la primera vez que se realiza la conexión con él. También puede iniciar el asistente de inicio rápido manualmente en cualquier momento.

*Para iniciar manualmente el asistente de inicio rápido, haga lo siguiente:*

1. En la ventana principal de la aplicación, haga clic en el icono de configuración (🔧) 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**.

3. Haga clic en **Iniciar asistente de inicio rápido**.

El asistente le solicita a realizar la configuración inicial del Servidor de administración. Siga las instrucciones del asistente. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

## 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 de bases de datos antivirus para Kaspersky Security Center Linux y las aplicaciones de Kaspersky administradas.

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 Linux con Internet.

- **Número de puerto** 

Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center Linux.

- **No utilizar 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, por separado del asistente de inicio rápido.

## Paso 2. Descargando actualizaciones requeridas

Las actualizaciones necesarias se descargan de los servidores de Kaspersky automáticamente.

## 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. Seleccione las opciones:

- [Áreas](#) <sup>?</sup>

Puede seleccionar los siguientes alcances de protección:

- **Estaciones de trabajo**
- **Servidores de archivos y almacenamiento**
- **Virtualización**
- **Sistemas integrados**
- **Redes industriales**
- **Endpoints industriales**

- [Sistemas operativos](#) <sup>?</sup>

Puede seleccionar las siguientes plataformas:

- Microsoft Windows
- macOS
- Android
- Linux
- Otro

Para obtener más información sobre sistemas operativos compatibles, consulte 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, por separado del 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.

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 se filtra de acuerdo con 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. La lista de complementos incluye las siguientes columnas:

- **Área para proteger** 

Las áreas seleccionadas para proteger 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 Linux que ha seleccionado en la instalación. Puede especificar otros idiomas en la lista desplegable **Mostrar el idioma de localización de la Consola de administración**.

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 usar 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 están instalados, el asistente de inicio rápido lo lleva automáticamente al siguiente paso.

## Paso 6. Descarga de paquetes de distribución y creación de paquetes de instalación

Seleccione los paquetes de distribución que desea descargar.

Las distribuciones de aplicaciones administradas pueden requerir la instalación de una versión mínima específica de Kaspersky Security Center Linux.

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 Linux. Si no existe un paquete de distribución de aplicaciones para el idioma Linux de Kaspersky Security Center Linux, se selecciona el paquete de distribución en inglés.

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 continuar con el siguiente paso del asistente, debe aceptar las condiciones del EULA y las 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.

## Paso 7. Configurar Kaspersky Security Network

Especifique la configuración para transmitir la información sobre las operaciones de Kaspersky Security Center Linux a la base de conocimientos de Kaspersky Security Network. Seleccione una de las siguientes opciones:

- [Acepto usar Kaspersky Security Network](#)

Kaspersky Security Center Linux 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 usar Kaspersky Security Network](#)

Kaspersky Security Center Linux 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 8. Selección del método de activación de la aplicación

Seleccione una de las siguientes opciones de activación de Kaspersky Security Center Linux:

- [Introducir su código de activación](#) 

Un *código de activación* es una secuencia única formada por 20 caracteres alfanuméricos. Introduzca un código de activación para añadir una clave que active Kaspersky Security Center Linux. Recibe el código de activación en la dirección de correo electrónico que especificó después de comprar Kaspersky Security Center.

Para activar la aplicación mediante un código de activación, se necesita acceso a Internet, ya que el proceso requiere comunicarse con los servidores de activación de Kaspersky.

Si ha seleccionado esta opción de activación, puede activar la opción **Desplegar clave de licencia automáticamente en dispositivos administrados**.

Si esta opción está habilitada, la clave de licencia se distribuirá automáticamente a los dispositivos administrados.

Si esta opción está desactivada, puede implementar la clave de licencia en los dispositivos administrados más adelante en la sección **Operaciones** → **Licencias** → **Licencias de Kaspersky** del menú principal.

- [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.

Recibe el archivo de clave en la dirección de correo electrónico que especificó después de comprar Kaspersky Security Center.

Para activar la aplicación con un archivo de clave, no es necesario conectarse a los servidores de activación de Kaspersky.

Si ha seleccionado esta opción de activación, puede activar la opción **Desplegar clave de licencia automáticamente en dispositivos administrados**.

Si esta opción está habilitada, la clave de licencia se distribuirá automáticamente a los dispositivos administrados.

Si esta opción está desactivada, puede implementar la clave de licencia en los dispositivos administrados más adelante en la sección **Operaciones** → **Licencias** → **Licencias de Kaspersky** del menú principal.

- Posponiendo la activación de aplicaciones

Si decide posponer la activación de la aplicación, puede agregar una clave de licencia más adelante en cualquier momento **Operaciones** → **Licencias**.



Cuando trabaja con Kaspersky Security Center desplegado desde una AML de pago o para un SKU facturado mensualmente según el uso, no puede especificar un archivo clave ni introducir un código.

## Paso 9. Creación de una configuración básica de protección de la red

Puede ver la lista de directivas y tareas creadas.

Espere a que se complete la creación de directivas y tareas antes de ir al paso siguiente del asistente.

## Paso 10. 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.

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.

- [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 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 el 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**.

## Paso 11. Cerrar el asistente de inicio rápido

Para cerrar el asistente, haga clic en el botón **Finalizar**.

Una vez que haya completado el asistente de inicio rápido, puede ejecutar el [asistente de despliegue de la protección](#) para instalar automáticamente aplicaciones antivirus o el Agente de red en los dispositivos de su red.

## 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 **Detección 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 en remoto**.

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.

## Iniciar Asistente de despliegue de la protección

También puede iniciar el asistente de despliegue de la protección manualmente en cualquier momento.

*Para iniciar manualmente el Asistente de despliegue de la protección,*

En el menú principal, vaya a **Detección y despliegue** → **Despliegue y asignación** → **Asistente de despliegue de la protección**.

Se inicia el Asistente de despliegue de la protección. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

## Paso 1. 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 **Añadir** y luego seleccione la aplicación en la lista.

## Paso 2. 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 añadir la 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**.

- [Añadir 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 3. 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 4. 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 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 resultarle útil para, por ejemplo, ejecutar una tarea en dispositivos que tengan una versión específica de un sistema operativo.

## Paso 5. Configurar la tarea de instalación remota

En la página **Configuración de tarea 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:

- [Usando 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.

- [Usando los recursos del sistema operativo mediante 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.

Esta opción se habilita de manera predeterminada para las tareas de instalación remota creadas en servidores de administración virtuales.

La única forma de instalar una aplicación para Windows (incluido el Agente de red para Windows) en un dispositivo que no tenga instalado el Agente de red es mediante un punto de distribución basado en Windows. Por lo tanto, cuando instale una aplicación de Windows:

- Seleccione esta opción.
- Asegúrese de que se asigne un punto de distribución para los dispositivos cliente de destino.
- Asegúrese de que el punto de distribución esté basado en Windows.

- [Usando los recursos del sistema operativo mediante el 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 habilitada de manera predeterminada.

Defina la configuración adicional:

#### **No reinstalar la aplicación si ya se encuentra 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 habilitada de manera predeterminada.

## Paso 6. 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 esta opción si desea que Kaspersky Security Center Linux 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 7. 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 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 dispositivos no asignados al grupo** 

Los dispositivos se moverán al grupo de administración que seleccione.

La opción **No mover dispositivos** está seleccionada de manera predeterminada. Es posible que quiera mover los dispositivos manualmente por seguridad.

## Paso 8. Seleccionar cuentas con acceso a los dispositivos

De ser necesario, agregue las cuentas que se utilizarán para iniciar la tarea de instalación remota:

- **No es necesaria una cuenta (Agente de red instalado)**<sup>?</sup>

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 ha instalado en los dispositivos cliente.

- **Se necesita una cuenta (para la instalación sin Agente de red)**<sup>?</sup>

Seleccione esta opción si el Agente de red no está instalado en los dispositivos a los que asigna la tarea de instalación remota. En ese caso, puede indicar una cuenta de usuario para instalar la aplicación.

Para especificar la cuenta de usuario con la que se ejecutará el instalador de la aplicación, haga clic en el botón **Añadir**, 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.

## Paso 9. Iniciar 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 tarea después de que finalice 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.

# Actualización de Kaspersky Security Center Linux

Puede instalar la versión 15 del Servidor de administración en un dispositivo que tenga instalada una versión anterior del Servidor de administración (a partir de la versión 13). Al actualizar a la versión 15, se conservan todos los datos y configuraciones de la versión anterior del Servidor de administración.

Antes de actualizar Kaspersky Security Center Linux, asegúrese de utilizar las versiones del sistema operativo y DBMS [compatibles con la versión 15 del Servidor de administración](#). Si es necesario, puede [mover el Servidor de administración a otro dispositivo](#) con versiones posteriores del sistema operativo y DBMS.

Puede actualizar una versión del Servidor de administración utilizando uno de los siguientes métodos:

- Mediante el [Archivo de instalación de Kaspersky Security Center Linux](#)
- Mediante la creación de la [Copia de seguridad de datos del Servidor de administración](#), la instalación de una nueva versión del Servidor de administración y la restauración de los datos del Servidor de administración desde la copia de seguridad

Durante la actualización, es fundamental que el DBMS no sea utilizado simultáneamente por el Servidor de administración y por otras aplicaciones.

Si su red incluye varios Servidores de administración, debe actualizar cada Servidor manualmente. Kaspersky Security Center Linux no admite la actualización centralizada.

Además, debe [actualizar Kaspersky Security Center Web Console](#) a una nueva versión.

Al actualizar Kaspersky Security Center Linux desde una versión anterior, se conservan todos los complementos instalados de las aplicaciones de Kaspersky compatibles. El complemento del Servidor de administración y el complemento del Agente de red se actualizan automáticamente. Recomendamos [crear una copia de seguridad de los datos del Servidor de administración](#) antes de iniciar la actualización.

## Actualización de Kaspersky Security Center Linux mediante el archivo de instalación

Para actualizar el Servidor de administración de una versión anterior (a partir de la versión 13) a la versión 15, puede instalar una nueva versión sobre una anterior mediante el archivo de instalación de Kaspersky Security Center Linux.

*Para actualizar una versión anterior del Servidor de administración a la versión 15 mediante el archivo de instalación:*

1. Descargue el archivo de instalación de Kaspersky Security Center Linux con un paquete completo para la versión 15 desde el sitio web de Kaspersky:

- Para dispositivos que ejecutan un sistema operativo basado en RPM: ksc64-<número de versión>.x86\_64.rpm
- Para dispositivos que ejecutan un sistema operativo basado en Debian: ksc64\_<número de versión>\_amd64.deb

2. Actualice el paquete de instalación mediante un administrador de paquetes que utilice en su Servidor de administración. Por ejemplo, puede usar los siguientes comandos en el terminal de línea de comandos en una cuenta con privilegios de root:

- Para dispositivos que ejecutan un sistema operativo basado en RPM:  
\$ sudo rpm -Uvh --nodeps --force ksc64-<número de versión>.x86\_64.rpm
- Para dispositivos que ejecutan un sistema operativo basado en Debian:  
\$ sudo dpkg -i ksc64-<número de versión>\_amd64.deb

Una vez que el comando se ha ejecutado correctamente, se crea el script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl. En la terminal se muestra el mensaje correspondiente.

3. Ejecute el script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl para configurar el Servidor de administración actualizado.

4. Lea el Contrato de licencia y la Política de privacidad, que aparecen en la terminal de línea de comandos. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad:

- Ingrese 'Y' para confirmar que ha leído, comprendido y aceptado en su totalidad los términos y condiciones del EULA.
- Ingrese 'Y' nuevamente para confirmar que ha leído, entendido y aceptado en su totalidad la Política de privacidad que describe el manejo de datos.

La instalación de la aplicación en su dispositivo continuará después de haber ingresado 'Y' dos veces.

5. Ingrese '1' para seleccionar el modo de instalación estándar del Servidor de administración.

La siguiente imagen muestra los dos últimos pasos.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

Aceptar los términos del EULA y la Política de privacidad, y seleccionar el modo de instalación estándar del Servidor de administración en el terminal de línea de comandos

A continuación, el script configura y finaliza la actualización del Servidor de administración. Durante la actualización, no puede cambiar los ajustes del Servidor de administración que haya configurado antes de la actualización.

6. Para dispositivos que tienen instalada una versión posterior 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 Linux.

La versión actualizada del Agente de red se instalará una vez que se complete la tarea de instalación remota.



## Actualizar Kaspersky Security Center Linux mediante copia de seguridad

Para actualizar el Servidor de administración de una versión anterior (a partir de la versión 13) a la versión 15, puede crear una copia de seguridad de los datos del Servidor de administración y restaurarlos después de instalar la nueva versión de Kaspersky Security Center Linux. Si se presentan problemas durante la instalación, puede restaurar la versión anterior del Servidor de administración usando la copia de seguridad del Servidor de administración creada antes de la actualización.

*Para actualizar una versión anterior del Servidor de administración a la versión 15 mediante copia de seguridad, realice lo siguiente:*

1. Antes de la actualización, [haga una copia de seguridad de los datos del Servidor de administración](#) con la versión anterior de la aplicación.
2. Desinstale la versión anterior de Kaspersky Security Center Linux.
3. [Instale Kaspersky Security Center Linux versión 15](#) en el anterior Servidor de administración.
4. [Restaure los datos del Servidor de administración](#) de la copia de seguridad creada antes de la actualización.
5. Para los dispositivos en los que estaba instalada la versión anterior del Agente de red, cree y ejecute la tarea para la instalación remota de 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 Linux.

La versión actualizada del Agente de red se instalará una vez que se complete la tarea de instalación remota.

## Actualización de Kaspersky Security Center Linux en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux

Puede instalar la versión 15 del Servidor de administración en cada nodo del clúster de conmutación por error de Kaspersky Security Center Linux que tenga instalada una versión anterior del Servidor de administración (a partir de la versión 14). Al actualizar a la versión 15, se conservan todos los datos y configuraciones de la versión anterior del Servidor de administración.

Si anteriormente instaló Kaspersky Security Center Linux en dispositivos localmente, también puede actualizar Kaspersky Security Center Linux en estos dispositivos mediante el [archivo de instalación](#) o [mediante una copia de seguridad](#).

*Para actualizar Kaspersky Security Center Linux en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux, haga lo siguiente:*

1. Descargue el archivo de instalación de Kaspersky Security Center Linux con un paquete completo para la versión 15 desde el sitio web de Kaspersky:
  - Para dispositivos que ejecutan un sistema operativo basado en RPM: ksc64-<número de versión>-<número de compilación>.x86\_64.rpm

- Para dispositivos que ejecutan un sistema operativo basado en Debian: ksc64\_<número de versión>-<número de compilación>\_amd64.deb

## 2. Detenga el clúster.

3. En el nodo activo del clúster, actualice el paquete de instalación mediante un administrador de paquetes que utilice en su Servidor de administración.

Por ejemplo, puede usar los siguientes comandos en el terminal de línea de comandos en una cuenta con privilegios de root:

- Para dispositivos que ejecutan un sistema operativo basado en RPM:  
\$ sudo rpm -Uvh --nodeps --force ksc64-<número de versión>-<número de compilación>.x86\_64.rpm
- Para dispositivos que ejecutan un sistema operativo basado en Debian:  
\$ sudo dpkg -i ksc64\_<número de versión>-<número de compilación>\_amd64.deb

Una vez que el comando se ha ejecutado correctamente, se crea el script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl. En la terminal se muestra el mensaje correspondiente.

4. Ejecute el script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl para configurar el Servidor de administración actualizado.
5. Lea el Contrato de licencia y la Política de privacidad, que aparecen en la terminal de línea de comandos. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad:

- a. Ingrese 'Y' para confirmar que ha leído, comprendido y aceptado en su totalidad los términos y condiciones del EULA.
- b. Ingrese 'Y' nuevamente para confirmar que ha leído, entendido y aceptado en su totalidad la Política de privacidad que describe el manejo de datos.

La instalación de la aplicación en su dispositivo continuará después de haber ingresado 'Y' dos veces.

6. Introduzca "2" para seleccionar el nodo en el que va a actualizar.

La siguiente imagen muestra los dos últimos pasos.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

Aceptar los términos del EULA y la Política de privacidad, y seleccionar el modo de instalación en el terminal de línea de comandos

A continuación, el script configura y finaliza la actualización del Servidor de administración. Durante la actualización, no puede cambiar los ajustes del Servidor de administración que haya configurado antes de la actualización.

7. Realice los pasos 3 a 5 en el nodo pasivo.

En el paso 6, introduzca "3" para seleccionar el nodo.

## 8. [Inicie el clúster.](#)

Tenga en cuenta que puede iniciar el clúster en cualquier nodo. Si inicia el clúster en el nodo pasivo, se convierte en el nodo activo.

Como resultado, ha instalado la versión más reciente del Servidor de administración en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux.

## Actualización de Kaspersky Security Center Web Console

En este artículo se describe cómo instalar el Servidor de Kaspersky Security Center Web Console Server (en lo sucesivo, también se usará la denominación "Kaspersky Security Center Web Console") en dispositivos con el sistema operativo Linux.

Si instala Kaspersky Security Center Web Console en Astra Linux en el modo de entorno de software cerrado, siga las [instrucciones específicas para Astra Linux](#).

Utilice uno de los siguientes archivos de instalación que corresponda a la distribución de Linux instalada en su dispositivo:

- Para Debian: ksc-web-console-[número\_de\_compilación].x86\_64.deb
- Para sistemas operativos basados en RPM: ksc-web-console-[número\_de\_compilación].x86\_64.rpm
- Para ALT 8 SP: ksc-web-console-[build\_number]-alt8p.x86\_64.rpm

El archivo de instalación debe descargarse del sitio web de Kaspersky.

*Para actualizar Kaspersky Security Center Web Console:*

1. Asegúrese de que el dispositivo en el que desea actualizar Kaspersky Security Center Web Console esté ejecutando una de las distribuciones de Linux compatibles.
2. Lea el Contrato de licencia de usuario final (EULA, por las siglas del término en inglés). Si el kit de distribución de Kaspersky Security Center Linux no incluye un archivo TXT con el texto del EULA, puede descargar el archivo desde el [sitio web de Kaspersky](#). Si no acepta los términos del Contrato de licencia, no actualice Kaspersky Security Center Web Console mediante el archivo de instalación.
3. Utilice el mismo [archivo de respuestas](#) que preparó antes de instalar Kaspersky Security Center Web Console. El nombre del archivo de respuesta es ksc-web-console-setup.json y la ubicación del archivo es /etc/ksc-web-console-setup.json.

Si el archivo de respuesta no existe, [cree un nuevo archivo de respuesta](#) que contenga los parámetros para conectar Kaspersky Security Center Web Console al Servidor de administración. Nombre el archivo ksc-web-console-setup.json y luego colóquelo en el directorio / etc.

Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros, y la dirección y el puerto predeterminados:

```
{
 "address": "127.0.0.1",
 "port": 8080,
```

```
"trusted":
"127.0.0.1|13299|/var/opt/kaspersky/klagent_srv/1093/cert/klserver.cer|KSC
Server",
"acceptEula": true
}
```

Si desea actualizar Kaspersky Security Center Web Console conectada al Servidor de administración instalado en los nodos del clúster de conmutación por error de Kaspersky Security Center Linux, en el [archivo de respuesta](#), especifique el parámetro de instalación de confianza para permitir que el clúster de conmutación por error de Kaspersky Security Center Linux se conecte a Kaspersky Security Center Web Console. El valor de cadena de este parámetro tiene el siguiente formato:

```
"trusted": "server address|port|certificate path|server name"
```

Especifique los componentes del parámetro de instalación trusted:

- **Dirección de Servidor de administración.** Si ha creado un adaptador de red secundario al [preparar los nodos del clúster](#), use la dirección IP del adaptador como la dirección del clúster de conmutación por error de Kaspersky Security Center Linux. De lo contrario, ingrese la dirección IP del equilibrador de carga de terceros que esté utilizando.
- **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 compartido del [clúster de conmutación por error de Kaspersky Security Center Linux](#). 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.
- **Nombre del Servidor de administración.** Es el nombre del clúster de conmutación por error de Kaspersky Security Center Linux que se mostrará en la ventana de inicio de sesión de Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console no se puede actualizar con el mismo archivo.rpm utilizado para la instalación. Si desea cambiar la configuración de un archivo de respuestas y usar este archivo para reinstalar la aplicación, primero debe eliminar la aplicación y luego volver a instalarla con el nuevo archivo de respuestas.

4. Con una cuenta con privilegios root, use la línea de comandos para ejecutar el archivo de instalación con la extensión .deb o .rpm, dependiendo de su distribución de Linux.

Para actualizar Kaspersky Security Center Web Console a una versión más reciente, ejecute uno de estos comandos:

- Para dispositivos que ejecutan un sistema operativo basado en RPM:  
\$ sudo rpm -Uvh --nodeps --force ksc-web-console-[ número\_de\_compilación ].x86\_64.rpm
- Para dispositivos que ejecutan un sistema operativo basado en Debian:  
\$ sudo dpkg -i ksc-web-console-[ número\_de\_compilación ].x86\_64.deb

Se iniciará el proceso para desempaquetar el archivo de instalación. Espere a que se complete la instalación.

5. Ejecute el siguiente comando para reiniciar todos los servicios de Kaspersky Security Center Web Console:  
\$ sudo systemctl restart KSC\*

Cuando finalice la instalación, puede usar su navegador para [abrir e iniciar sesión en Kaspersky Security Center Web Console](#).

## Instalar Kaspersky Security Center Web Console en Astra Linux en el modo de entorno de software cerrado

En esta sección, se describe cómo instalar el Servidor de Kaspersky Security Center Web Console Server (en lo sucesivo, también se usará la denominación "Kaspersky Security Center Web Console") en el sistema operativo Astra Linux Special Edition.

*Para actualizar Kaspersky Security Center Web Console:*

1. Asegúrese de que el dispositivo en el que desea actualizar Kaspersky Security Center Web Console esté ejecutando una de las distribuciones de Linux compatibles.
2. Lea el Contrato de licencia de usuario final (EULA, por las siglas del término en inglés). Si el kit de distribución de Kaspersky Security Center Linux no incluye un archivo TXT con el texto del EULA, puede descargar el archivo desde el [sitio web de Kaspersky](#). Si no acepta los términos del Contrato de licencia, no actualice Kaspersky Security Center Web Console mediante el archivo de instalación.
3. Utilice el mismo [archivo de respuestas](#) que preparó antes de instalar Kaspersky Security Center Web Console. El nombre del archivo de respuesta es `ksc-web-console-setup.json` y la ubicación del archivo es `/etc/ksc-web-console-setup.json`.

Si el archivo de respuesta no existe, [cree un nuevo archivo de respuesta](#) que contenga los parámetros para conectar Kaspersky Security Center Web Console al Servidor de administración. Nombre el archivo `ksc-web-console-setup.json` y luego colóquelo en el directorio `/etc`.

Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros, y la dirección y el puerto predeterminados:

```
{
 "address": "127.0.0.1",
 "port": 8080,
 "trusted":
 "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
 Server",
 "acceptEula": true
}
```

4. Asegúrese de que en el archivo `/etc/digisig/digisig_initramfs.conf`, el parámetro `DIGSIG_ELF_MODE` se especifique de la siguiente manera:

```
DIGSIG_ELF_MODE=1
```

5. Asegúrese de que el paquete de compatibilidad `astra-digisig-oldkeys` esté instalado.

Si este paquete no está instalado, ejecute el siguiente comando:

```
apt install astra-digisig-oldkeys
```

6. Cree un directorio para la clave de la aplicación, si no existe:

```
mkdir -p /etc/digisig/keys/legacy/kaspersky/
```

7. Coloque la clave de la aplicación `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` en el directorio creado en el paso anterior:

```
cp kaspersky_astra_pub_key.gpg /etc/digisig/keys/legacy/kaspersky/
```

Si el kit de distribución de Kaspersky Security Center Linux no incluye la clave de la aplicación kaspersky\_astra\_pub\_key.gpg, puede descargarla haciendo clic en el enlace:

[https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky\\_astra\\_pub\\_key.gpg](https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg).

8. Actualice los discos RAM:

```
update-initramfs -u -k all
```

Reinicie el sistema.

9. En una cuenta con privilegios de raíz, utilice la línea de comandos para ejecutar el archivo de instalación. El archivo de instalación debe descargarse del sitio web de Kaspersky.

Para actualizar Kaspersky Security Center Web Console a una versión más reciente, ejecute el siguiente comando:

```
$ sudo dpkg -i ksc-web-console-[número_de_compilación].x86_64.deb
```

Se iniciará el proceso para desempaquetar el archivo de instalación. Espere a que se complete la instalación.

10. Ejecute el siguiente comando para reiniciar todos los servicios de Kaspersky Security Center Web Console:

```
$ sudo systemctl restart KSC*
```

Cuando finalice la instalación, puede usar su navegador para [abrir e iniciar sesión en Kaspersky Security Center Web Console](#).

# Migración a Kaspersky Security Center Linux

Si sigue 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.

Limitaciones:

- La migración solo es posible de Kaspersky Security Center 14.2 Windows a Kaspersky Security Center 15.0 Linux.
- Puede realizar estas acciones solo mediante Kaspersky Security Center Web Console.

Antes de comenzar, obtenga más información sobre las funciones y las limitaciones de Kaspersky Security Center Linux:

- [Diferencias funcionales entre Kaspersky Security Center Windows y Kaspersky Security Center Linux](#)
- [Lista de aplicaciones de Kaspersky compatibles con Kaspersky Security Center Linux](#)

## Etapas

El escenario de migración avanza en etapas:

### 1 Escoja un método de migración

Migre 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 administra el proceso de migración y cambia entre Servidores dentro de una sola instancia de Kaspersky Security Center Web Console. Si prefiere esta opción, puede organizar los Servidores de administración en una jerarquía a fin de 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. El proceso de migración se administra con dos instancias de Kaspersky Security Center Web Console: una instancia para Kaspersky Security Center Windows y otra para Kaspersky Security Center Linux. En este caso, utilizará el archivo de exportación que ha creado y descargado durante la [exportación desde Kaspersky Security Center Windows](#) e [importará este archivo a Kaspersky Security Center Linux](#).

### 2 Exporte datos desde Kaspersky Security Center Windows

Abra Kaspersky Security Center Windows y, luego, ejecute el [Asistente de migración](#).

### 3 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.

#### 4 Realice acciones adicionales para transferir objetos y configuraciones desde Kaspersky Security Center Windows a Kaspersky Security Center Linux de forma manual (paso opcional)

También es posible que desee 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 utiliza 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](#)

#### 5 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. En la versión actual de Kaspersky Security Center Linux, puede hacerlo mediante uno de los siguientes métodos:

- Mediante la [utilidad klmove](#)  
Use la utilidad klmove 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. Use el paquete de instalación para instalar el Agente de red en los dispositivos administrados importados a través de una [tarea de instalación remota](#). Para obtener más información, consulte [Cambio de dispositivos administrados bajo la administración de Kaspersky Security Center Linux](#).  
También puede crear y usar 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 para Linux](#) a la misma versión que Kaspersky Security Center.

#### 7 Asegúrese de que los dispositivos administrados sean 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 está instalado** y **Última conexión al Servidor de administración**.

## Otros métodos de migración de datos

Además del asistente de migración, existen otros métodos para transferir los objetos actuales, pero solo permiten transferir tareas y directivas:



- [Exporte las tareas](#) desde Kaspersky Security Center Windows y, a continuación, [impórtelas](#) a Kaspersky Security Center Linux.
- [Exporte directivas específicas](#) desde Kaspersky Security Center Windows y, a continuación, [importe las directivas](#) a Kaspersky Security Center Linux. Los perfiles de directivas relacionadas se exportan e importan junto con las directivas seleccionadas.

## 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: usando o no la jerarquía de Servidores de administración de Kaspersky Security Center Windows y Kaspersky Security Center Linux.

*Para exportar dispositivos administrados y objetos relacionados a través del Asistente de migración, siga estos pasos:*

1. Dependiendo de si los Servidores de administración de Kaspersky Security Center Windows y Kaspersky Security Center Linux están organizados en una jerarquía, realice una de las siguientes acciones:
  - Si los servidores están organizados en una jerarquía, abra Kaspersky Security Center Web Console y luego cambie al servidor de Kaspersky Security Center Windows.
  - Si los servidores no están organizados en una jerarquía, abra Kaspersky Security Center Web Console conectado a Kaspersky Security Center Windows.
2. En el menú principal, vaya a **Operaciones** → **Migración**.
3. Seleccione **Migrar a Kaspersky Security Center Linux o Kaspersky Single Management Platform** para iniciar el asistente y siga los pasos.
4. Seleccione el grupo o subgrupo de administración que desea exportar. Asegúrese de que el grupo o subgrupo de administración seleccionado no contenga más de 10 000 dispositivos.
5. Seleccione las aplicaciones administradas cuyas tareas y directivas se exportarán. Seleccione solo las aplicaciones compatibles con Kaspersky Security Center Linux. Los objetos de las aplicaciones no compatibles

se seguirán exportando, pero no estarán operativos.

6. Utilice los enlaces de la izquierda para seleccionar las tareas globales, las selecciones de dispositivos y los informes para exportar. El enlace **Objetos de grupo** le permite excluir funciones personalizadas, usuarios internos y grupos de seguridad, y categorías de aplicaciones personalizadas de la exportación.

Se crea el archivo de exportación (archivo ZIP). Según 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 el archivo de exportación guardado a Kaspersky Security Center Linux manualmente](#).

## Importación del archivo de exportación en Kaspersky Security Center Linux

Para transferir información sobre dispositivos administrados, objetos y sus configuraciones que [ha exportado desde Kaspersky Security Center Windows](#), debe importarla a Kaspersky Security Center Linux o Kaspersky XDR Expert.

*Para importar dispositivos administrados y objetos de grupo relacionados a través del Asistente de migración, siga estos pasos:*

1. Dependiendo de si los Servidores de administración de Kaspersky Security Center Windows y Kaspersky Security Center Linux están organizados en una jerarquía, realice una de las siguientes acciones:
  - Si los Servidores están organizados en una jerarquía, continúe con el siguiente paso del Asistente de migración una vez que se complete la exportación. La importación se inicia 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 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 inicia 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 enlace **Cambiar** y, luego, elija el archivo requerido.
3. Se muestra toda la jerarquía de grupos de administración de Kaspersky Security Center Linux.  
Seleccione la casilla junto al grupo de administración de destino al que se deben restaurar los objetos del grupo de administración exportado (dispositivos administrados, directivas, tareas y otros objetos de grupo).
4. Se inicia 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 iconos de actualización (↻) junto a todos los

elementos de la lista de objetos se reemplacen con marcas de verificación color verde (✓) y finalice la importación.

5. Cuando termina la importación, la estructura exportada de los grupos de administración, incluidos los detalles del dispositivo, aparece debajo del grupo de administración de destino que ha seleccionado. Si el nombre del objeto que desea restaurar es idéntico al nombre de un objeto existente, al primero se le añade un sufijo progresivo.

Si en una tarea que ha migrado [se especifican los detalles de la cuenta bajo la cual se ejecuta la tarea](#), debe abrir la tarea y volver a ingresar la contraseña tras completarse la importación.

Si la importación se ha completado con un error, puede realizar una de las siguientes acciones:

- Para una migración compatible con la jerarquía del Servidor de administración, puede comenzar a importar de nuevo el archivo de exportación.
- Para una migración no compatible con la jerarquía del Servidor de administración, puede iniciar el Asistente de migración para seleccionar otro archivo de exportación y luego volver a importarlo.

Puede comprobar si los objetos de grupo incluidos en el alcance de la exportación se importaron correctamente a Kaspersky Security Center Linux. Para ello, diríjase 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 no está instalado ni ejecutándose en ellos (el valor *No* en las columnas **Visible**, **Agente de red está instalado** y **Agente de red está en ejecución**).

Para completar la migración, debe [cambiar los dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux](#).

## Cambio de 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.

En la versión actual de Kaspersky Security Center Linux puede mover los dispositivos administrados para que estén bajo la administración de Kaspersky Security Center Linux mediante la [utilidad klmover](#) o instalando el 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, siga estos pasos:*

1. Cambie al Servidor de administración de Kaspersky Security Center Windows.
2. Vaya a **Detección 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](#).

3. En la pestaña **Configuración**, seleccione la sección **Conexión**. Especifique la configuración de conexión del Servidor de administración de Kaspersky Security Center Linux.

4. Cree una [tarea de instalación remota](#) para los 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 de un dispositivo basado en Windows que actúa como [punto de distribución](#). Si utiliza el Servidor de administración, active la opción **Usando los recursos del sistema operativo mediante el Servidor de administración**. Si utiliza un punto de distribución, active la opción **Usando los recursos del sistema operativo mediante puntos de distribución**.

5. Ejecute la tarea de instalación remota.

Después de que la tarea de instalación remota finalice correctamente, vaya al Servidor de administración de Kaspersky Security Center Linux y asegúrese de que los dispositivos administrados sean visibles en la red y que el Agente de red esté instalado y ejecutándose en ellos (el valor *Sí* en las columnas **Visible**, **Agente de red está instalado** y **Agente de red está en ejecución**).

## 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.

## Configurar una lista de direcciones IP permitidas para iniciar sesión en Kaspersky Security Center Linux

De manera predeterminada, los usuarios pueden iniciar sesión en Kaspersky Security Center Linux desde cualquier dispositivo en el que puedan abrir Kaspersky Security Center Web Console. Si lo desea, puede hacer que el Servidor de administración únicamente acepte conexiones de dispositivos que tengan una dirección IP permitida. En este caso, incluso si un intruso roba una cuenta de Kaspersky Security Center Linux, no podrá iniciar sesión en Kaspersky Security Center Linux porque la dirección IP del dispositivo del intruso no está en la lista de permitidos.

La dirección IP se verifica cuando un usuario inicia sesión en Kaspersky Security Center Linux o ejecuta una [aplicación](#) que interactúa con el Servidor de administración a través de [Kaspersky Security Center Linux OpenAPI](#). 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 admitidos, se produce un error de autenticación y el [evento KLAUD\\_EV\\_SERVERCONNECT](#) notifica que no se ha establecido una 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 Kaspersky Security Center Web Console

Si inicia sesión en Kaspersky Security Center Linux a través de Kaspersky Security Center Web Console, puede configurar un firewall en el dispositivo donde está instalado el Servidor de Kaspersky Security Center Web Console utilizando los medios estándar del sistema operativo. Después, si alguien intenta iniciar sesión en Kaspersky Security Center Linux en un dispositivo y el Servidor de Kaspersky Security Center Web Console está [instalado en otro dispositivo](#), un firewall ayuda a evitar que los intrusos interfieran.

- Aplicaciones que interactúan con el Servidor de administración a través de objetos de automatización de klakout
- 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 establecer la lista de direcciones IP permitidas para iniciar sesión en Kaspersky Security Center Linux, haga lo siguiente:*

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 su directorio actual a la carpeta de instalación de Kaspersky Security Center Linux (normalmente, /opt/kaspersky/ksc64/sbin).

3. Introduzca el siguiente comando en la cuenta raíz:

```
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.

Puede averiguar si configuró correctamente la lista de direcciones IP permitidas en el Registro de eventos de Syslog 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. Introduzca el siguiente comando en el símbolo del sistema en la cuenta raíz:

```
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.

## 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 de bases de datos antivirus para Kaspersky Security Center Linux 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 icono de configuración (⚙️) 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 del 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 Linux con Internet.

- [Número de puerto](#) ⓘ

Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center Linux.

- [No utilizar 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](#).

## Jerarquía de Servidores de administración

Algunas empresas cliente, por ejemplo MSP, pueden ejecutar varios Servidores de administración. Puede ser poco conveniente administrar varios Servidores de administración independientes, por lo que se puede aplicar una jerarquía. En una jerarquía, un Servidor de administración basado en Linux puede funcionar tanto como Servidor principal como Servidor secundario. El servidor principal basado en Linux puede administrar tanto servidores secundarios basados en Linux como basados en Windows. Un servidor principal basado en Windows puede administrar un servidor secundario basado en Linux.

La configuración "principal/secundario" de dos Servidores de administración proporciona las opciones siguientes:

- Un Servidor de administración secundario hereda directivas, tareas, funciones de usuario y paquetes de instalación del Servidor de administración principal, lo que evita la copia de la configuración.
- 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.
- Un Servidor de administración principal se puede usar como origen de actualizaciones para un Servidor de administración secundario.

El Servidor de administración principal solo recibe datos de Servidores de administración secundarios no virtuales dentro del alcance de las opciones enumeradas anteriormente. Esta limitación no se aplica a los Servidores de administración virtuales, que comparten la base de datos con su Servidor de administración principal.

## Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario



En una jerarquía, un Servidor de administración basado en Linux puede funcionar tanto como Servidor principal como Servidor secundario. El servidor principal basado en Linux puede administrar tanto servidores secundarios basados en Linux como basados en Windows. Un servidor principal basado en Windows puede administrar un servidor secundario basado en Linux.

## 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, haga clic en 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 añadir un Servidor de administración secundario.
6. En la primera página del asistente, complete los siguientes campos:

- [Nombre a 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.

- [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 el 13000.

- [Puerto 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 el 13299.

- [Conectar Servidor de administración principal a 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, 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.

- [Usar servidor proxy](#) 

Seleccione esta opción si utiliza un servidor proxy para conectarse al Servidor de administración secundario.

En este caso, también tiene que especificar la siguiente configuración del servidor proxy:

- **Dirección**
- **Nombre de usuario**
- **Contraseña**

## 7. 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.

## 8. Ingrese las credenciales de un usuario que tenga derechos para acceder al futuro Servidor de administración secundario.

Asegúrese de que la verificación en dos pasos esté deshabilitada para la cuenta que indique. Si la verificación en dos pasos está habilitada para esta cuenta, solamente podrá crear la jerarquía desde el futuro Servidor secundario (encontrará instrucciones para ello más abajo). La empresa está [al tanto de este problema](#).

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 también puede fallar porque el futuro Servidor secundario se autentique con un certificado autofirmado generado automáticamente por Kaspersky Security Center Linux. En tal caso, el navegador podría bloquear la descarga del certificado autofirmado. Si se presenta este problema, puede realizar una de las siguientes acciones:

- Cree un certificado para el futuro Servidor secundario que se considere de confianza en su infraestructura y que cumpla con los [requisitos para certificados personalizados](#).
- Agregue el certificado autofirmado del futuro Servidor secundario a la lista de certificados de confianza del navegador. Recomendamos que utilice esta opción solo si no puede crear un certificado personalizado. Para obtener información sobre cómo agregar un certificado a la lista de certificados de confianza, consulte la documentación de su navegador.

Una vez que el asistente termina, se crea la jerarquía "principal/secundario". 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 estaba temporalmente desconectado o no estaba disponible, o porque el archivo de certificado del Servidor de administración secundario es autofirmado), aún puede añadir 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 del certificado se encuentra en el futuro Servidor de administración principal, en `/var/opt/kaspersky/klhagent_srv/1093/cert/`.

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 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 Servidor de administración principal a Servidor de administración secundario en DMZ**.
- g. Si la conexión con el futuro Servidor de administración principal 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 recibiendo conexión del Servidor de administración secundario a través del 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 donde está instalado Kaspersky Security Center Web Console, ejecute el archivo de instalación de Kaspersky Security Center Web Console correspondiente a la distribución de Linux instalada en su dispositivo con una cuenta con privilegios administrativos.
2. Se iniciará el asistente de instalación.
3. En la primera página del asistente, seleccione la opción **Actualizar**.
4. En la página **Tipo de modificación**, seleccione la opción **Editar la configuración de conexión**.
5. En la página **Servidores de administración de confianza**, agregue el Servidor de administración secundario necesario.
6. En la última página del asistente, haga clic en **Modificar** para aplicar la nueva configuración.
7. 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](#) donde se ha creado el servidor virtual. Una vez que haga esto, podrá cambiar al Servidor de administración virtual en Kaspersky Security Center Web Console.

## 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.

*Para crear y agregar un Servidor de administración virtual:*

1. En el menú principal, haga clic en el ícono 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 del 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 donde está instalado Kaspersky Security Center Web Console, ejecute el archivo de instalación de Kaspersky Security Center Web Console correspondiente a la distribución de Linux instalada en su dispositivo con una cuenta con privilegios administrativos.
2. Se iniciará el asistente de instalación.
3. En la primera página del asistente, seleccione la opción **Actualizar**.
4. En la página **Tipo de modificación**, seleccione la opción **Editar la configuración de conexión**.
5. En la página **Servidores de administración de confianza**, agregue el Servidor de administración secundario necesario.
6. En la última página del asistente, haga clic en **Modificar** para aplicar la nueva configuración.
7. 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](#) donde se ha creado el servidor virtual. Una vez que haga esto, podrá cambiar al Servidor de administración virtual en Kaspersky Security Center Web Console.

## 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 ícono 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 **Activar/Desactivar 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. Por ejemplo, esto puede ser útil cuando crea Servidores de administración virtuales para administrar oficinas o departamentos separados de su organización, o si es un proveedor de servicios administrados (MSP) y administra sus inquilinos a través de Servidores de administración 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 una o más funciones de usuario para el administrador

Para [iniciar sesión en Kaspersky Security Center Web Console](#), un administrador de un Servidor de administración virtual especifica el nombre, el nombre de usuario y la contraseña del Servidor de administración virtual. Kaspersky Security Center Web Console autentica el administrador y abre el Servidor de administración virtual al que el administrador tiene derechos de acceso. 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 objetos](#) en el área funcional **Funciones 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 requerido:
  - a. Haga clic en el icono de flecha () a la derecha del nombre del Servidor de administración actual.
  - b. Seleccione el Servidor de administración requerido.
2. En la ventana principal de la aplicación, haga clic en el icono de configuración () 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 **Añadir**  
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 añade el usuario seleccionado a la lista de usuarios en la pestaña **Derechos de acceso**.

5. Seleccione la casilla de verificación junto a la cuenta añadida y, a continuación, 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, como mínimo, los siguientes derechos:

- Derecho **Leer** en el área funcional **Funciones generales** → **Funcionalidad básica**
- Derecho de **Leer** en el área funcional **Funciones generales** → **Servidores de administración virtual**

La aplicación guarda los derechos de usuario modificados en la cuenta de administrador.

## Configurar derechos de acceso mediante la asignación de funciones de usuario

De forma alternativa, puede otorgar los derechos de acceso a un administrador del Servidor de administración virtual a través de funciones 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 funciones 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 funciones de usuario:*

1. En el Servidor de administración principal, [cree una nueva función 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 varias funciones, por ejemplo, si desea separar el acceso a diferentes áreas funcionales.
2. En el menú principal, cambie al Servidor de administración virtual requerido:
  - a. Haga clic en el icono de flecha (▾) a la derecha del nombre del Servidor de administración actual.
  - b. Seleccione el Servidor de administración requerido.
3. [Asigne la nueva función o varias funciones a la cuenta de administrador](#).

La aplicación asigna las funciones a la cuenta de 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. El cambio de mando puede realizarse entre los siguientes servidores de administración:





- El Servidor de administración principal y uno de sus servidores administración virtuales
- Dos servidores de administración virtuales pertenecientes a un mismo Servidor de administración principal

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 **Añadir**.  
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 **Cambiar 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. Seleccione los dispositivos a los que se asignará la tarea.
6. Seleccione el Servidor de administración que desee utilizar para administrar los dispositivos seleccionados.
7. 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 manera 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 habilita la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**, podrá modificar la configuración predeterminada 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.
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 devolver los dispositivos en la administración de Kaspersky Security Center Linux, ejecute el sondeo de red y luego mueva los dispositivos encontrados del grupo de Dispositivos no asignados a los grupos de administración.

*Para eliminar un Servidor de administración virtual:*

1. En la ventana principal de la aplicación, haga clic en el icono de configuración (⚙️) 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.

## 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 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 icono 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 conexión del Servidor de administración**.

Todos los eventos adicionales de las conexiones entrantes con el Servidor de administración, los resultados de autenticación y los errores de SSL se guardarán en el archivo `/var/opt/kaspersky/klnagent_srv/logs/sc.syslog`.

## 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 conservar solo la cantidad máxima especificada de eventos.

Cuando el Servidor de administración elimina los eventos antiguos, no puede guardar los nuevos eventos en la base de datos. Durante este período, la información sobre los eventos que se rechazaron se escribe en el registro del sistema operativo. 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**.

## 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.
- 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, puede ejecutar la [tarea de copia de seguridad de datos](#) a través de Kaspersky Security Center Web Console o ejecutar la [utilidad klbackup](#).

2. 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.

3. En el nuevo dispositivo, [instale el DBMS](#) que utilizará el Servidor de administración.

Cuando seleccione un DBMS, tenga en cuenta la cantidad de dispositivos cubiertos por el Servidor de administración.

4. Instale el Servidor de administración en el nuevo dispositivo.

Tenga en cuenta que si mueve el servidor de la base de datos al nuevo dispositivo, debe especificar la dirección local como la dirección IP del dispositivo en el que está instalada la base de datos (el elemento "h" en la instrucción [Instalación de Kaspersky Security Center Linux](#)). Si necesita mantener el servidor de la base de datos en el dispositivo anterior, introduzca la dirección IP del dispositivo anterior en el elemento "h" de la instrucción [Instalar Kaspersky Security Center Linux](#).

5. Una vez completada la instalación, recupere los datos del Servidor de administración en el nuevo dispositivo mediante la utilidad kbackup.

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.

6. Abra Kaspersky Security Center Web Console y [conéctese al Servidor de administración](#).

7. Verifique que todos los dispositivos del cliente estén conectados al Servidor de administración.

8. Desinstale el Servidor de administración y el servidor de la base de datos del dispositivo anterior.

## Cambio de las credenciales de DBMS

Es posible que, a veces, 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 Linux mediante la utilidad klsrvswch.exe:*

1. Inicie una línea de comando de Linux.

2. Especifique la utilidad klsrvconfig en la ventana de línea de comando abierta:

```
sudo /opt/kaspersky/ksc64/sbin/klsvconfig -set_dbms_cred
```

3. Especifique un nuevo nombre de cuenta. Debe especificar las credenciales de una cuenta que exista en el DBMS.

4. Introduzca una nueva contraseña.

5. Especifique la nueva contraseña para su confirmación.

Se cambian las credenciales de la DBMS.

## 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 los datos tras mover la base de datos del Servidor de administración a otro dispositivo o al actualizar a una versión más reciente de Kaspersky Security Center Linux (no se admite mover los datos del Servidor de administración para que estén bajo la administración de Kaspersky Security Center Windows).

Tenga en cuenta que 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, compruebe si se añade un Servidor de administración virtual al grupo de administración. Si se añade un Servidor de administración virtual, asegúrese de que [se asigne un administrador](#) a este Servidor de administración virtual antes de crear la copia de seguridad. No puede otorgar al administrador los derechos de acceso al Servidor de administración virtual después de crear 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 administración virtual.

Puede crear una copia de seguridad de los datos del Servidor de administración mediante uno de los siguientes métodos:

- Creando y ejecutando un [tarea de copia de seguridad de datos](#) a través de Kaspersky Security Center Web Console.
- 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. Después de la instalación del Servidor de administración, la utilidad se ubica en la raíz de la carpeta de destino especificada durante la instalación de la aplicación (por lo general, /opt/kaspersky/ksc64/sbin/klbackup).

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.

La recuperación de los datos del Servidor de administración solo se puede realizar mediante la utilidad klbackup.

## Crear una tarea de creación de copias de seguridad de los datos del Servidor de administración:

Las tareas de creación de copias de seguridad son tareas del Servidor de administración creadas por el [asistente de inicio rápido](#). Si se ha eliminado una tarea de creación de copias de seguridad creada por el asistente de inicio rápido, puede crear una manualmente.

La tarea *Copia de seguridad de los datos del Servidor de administración* solo puede crearse en una sola copia. Si la tarea de creación de copias de seguridad de los datos del Servidor de administración ya se ha creado, no aparecerá en la ventana de selección de tipo de tarea.

*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 **Añadir**.  
Se inicia el Asistente para crear nueva tarea.
3. En la primera página del asistente, en la lista **Aplicación**, seleccione **Kaspersky Security Center 15**, y 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:
  - Carpeta para el almacenamiento de copias de seguridad
  - Contraseña de la copia de seguridad (opcional)
  - Número máximo de copias de seguridad para guardar
5. Si habilita la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**, podrá modificar la configuración predeterminada 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 y se la agrega a la lista de tareas.

## Uso de la utilidad klbackup para realizar copias de seguridad y recuperar datos

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.

*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.

Sintaxis de línea de comandos de la utilidad:

```
k1backup -path BACKUP_PATH [-logfile LOGFILE] [-use_ts][[-restore] [-password PASSWORD] [-online]
```

Si no se especificó una contraseña en la línea de comandos de la utilidad k1backup, la utilidad solicitará que se ingrese la contraseña de modo interactivo.

Descripciones de las claves:

- `-path BACKUP_PATH`: Guardar información en la carpeta `BACKUP_PATH` o usar datos de la carpeta `BACKUP_PATH` para la recuperación (parámetro obligatorio).
- `-logfile LOGFILE`: Guardar un informe sobre la copia de seguridad y recuperación de datos del Servidor de administración.

La cuenta del servidor de bases de datos y la utilidad k1backup deben contar con permisos para modificar los datos de la carpeta `BACKUP_PATH`.

- `-use_ts`: para guardar datos, copiar la información en la carpeta `BACKUP_PATH`, en la subcarpeta con un nombre que contenga la hora y fecha de la operación del sistema actual en formato `k1backup YYYY-MM-DD # HH-MM-SS`. Si no se especifica una clave, la información se guarda en la raíz de la carpeta `BACKUP_PATH`.

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 `k1backup 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 partir de la información almacenada en la carpeta `BACKUP_PATH`. Si no se dispone de una clave, se crea una copia de seguridad de los datos en la carpeta `BACKUP_PATH`.
- `-password PASSWORD`: guardar o recuperar el certificado del Servidor de administración; para cifrarlo o descifrarlo, utilice la contraseña especificada en el parámetro `PASSWORD`.

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 k1backup debe tener acceso completo a la carpeta compartida. Recomendamos que ejecute la utilidad en un Servidor de administración recién instalado.

- `-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.

## 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.

La tarea Mantenimiento del Servidor de administración no es compatible con MariaDB. Si se utiliza este DBMS en su red, los administradores deberán mantener MariaDB por su cuenta.

La tarea Mantenimiento del Servidor de administración se crea automáticamente al instalar Kaspersky Security Center Linux. 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 **Añadir**.  
Se inicia el Asistente para crear nueva tarea.
3. En la ventana **Nueva tarea** 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 ya ha creado una tarea Mantenimiento del Servidor de administración para un Servidor de administración, no podrá crear una nueva tarea Mantenimiento del Servidor de administración.

## 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 icono de configuración (⚙️) 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.

## Acceso a los servidores de DNS públicos

Si no es posible acceder a los servidores de Kaspersky mediante el DNS del sistema, Kaspersky Security Center Linux puede utilizar estos servidores DNS públicos en el siguiente orden:

1. DNS público de Google (8.8.8.8)
2. DNS de Cloudflare (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

Las solicitudes 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 el servidor DNS. Si Kaspersky Security Center Linux utiliza un servidor DNS público, el procesamiento de datos se rige por la política de privacidad del servicio correspondiente.

*Para configurar el uso de DNS público mediante la utilidad `klscflag`:*

1. Ejecute el símbolo del sistema y luego cambie el directorio actual al directorio con la utilidad `klscflag`. La utilidad `klscflag` se encuentra en el directorio donde está instalado el Servidor de administración. La ruta de instalación predeterminada es `/opt/kaspersky/ksc64/sbin`.
2. Para desactivar el uso de DNS público, introduzca el siguiente comando en la cuenta root:  

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
```
3. Para activar el uso de DNS público, introduzca el siguiente comando en la cuenta root:  

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
```

## 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, elija **Opciones de interfaz**.
2. En la ventana **Opciones de interfaz** que se abre, active o desactive la opción **Mostrar protección y cifrado de datos**.
3. Haga clic en **Guardar**.

Después de eso, la sección **Operaciones** → **Protección y cifrado de datos** aparece en el menú principal.

## Cifrar la comunicación con TLS

Para corregir vulnerabilidades en la red corporativa de su organización, puede activar el cifrado de tráfico mediante el protocolo TLS. Puede activar los protocolos de cifrado TLS y los conjuntos de cifrado compatibles en el Servidor de administración. Kaspersky Security Center Linux 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 Linux utiliza certificados autofirmados. También puede utilizar sus propios certificados. Los especialistas de Kaspersky recomiendan utilizar certificados emitidos por autoridades de certificación de confianza.

*Para configurar los protocolos de cifrado permitidos y las suites de cifrado en el Servidor de administración:*

1. Ejecute el símbolo del sistema y luego cambie el directorio actual al directorio con la utilidad `klscflag`. La utilidad `klscflag` se encuentra en el directorio donde está instalado el Servidor de administración. La ruta de instalación predeterminada es `/opt/kaspersky/ksc64/sbin`.
2. Utilice el indicador `SrvUseStrictSslSettings` para configurar los protocolos y los conjuntos de cifrado permitidos en el Servidor de administración. Ejecute el siguiente comando en la línea de comandos en la cuenta raíz:

```
klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <valor> -t d
```

Especifique el parámetro `<valor>` del indicador `SrvUseStrictSslSettings` flag:

- 4: Solo están activados los protocolos TLS 1.2 y TLS 1.3. También se activan 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 11). 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 activados los protocolos TLS 1.2 y TLS 1.3. Para los protocolos 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 (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 Linux:

- Servidor de administración
- Servidor web
- Proxy de activación

Como resultado, se activa el cifrado de tráfico mediante el protocolo TLS.

Puede utilizar los indicadores KLTR\_TLS12\_ENABLED y KLTR\_TLS13\_ENABLED para activar la compatibilidad con los protocolos TLS 1.2 y TLS 1.3, respectivamente. Estos indicadores están activados de forma predeterminada.

*Para activar o desactivar la compatibilidad con los protocolos TLS 1.2 y TLS 1.3, siga estos pasos:*

1. Ejecute la utilidad klscflag.

Ejecute el símbolo del sistema y luego cambie el directorio actual al directorio con la utilidad klscflag. La utilidad klscflag se encuentra en el directorio donde está instalado el Servidor de administración. La ruta de instalación predeterminada es /opt/kaspersky/ksc64/sbin.

2. Ejecute uno de los siguientes comandos en la línea de comandos en la cuenta raíz:

- Utilice este comando para activar o desactivar la compatibilidad con el protocolo TLS 1.2:

```
klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v
<value> -t d
```

- Utilice este comando para activar o desactivar la compatibilidad con el protocolo TLS 1.3:

```
klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v
<value> -t d
```

Especifique el parámetro <valor> del indicador:

- 1: Para activar la compatibilidad con el protocolo TLS.
- 0: Para desactivar la compatibilidad con el protocolo TLS.

# Descubrimiento de dispositivos conectados a la red

Esta sección describe la búsqueda y la detección de dispositivos conectados a una red.

Kaspersky Security Center Linux permite encontrar dispositivos según los 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. Descubrir qué dispositivos están conectados a la red le permitirá recibir información sobre ellos y usar directivas para administrarlos. La red debe sondearse en forma periódica tanto para detectar dispositivos nuevos como para determinar si los ya descubiertos siguen conectados.

El proceso para descubrir los dispositivos conectados a la red se divide en etapas:

### 1 Descubrimiento de dispositivos inicial

Cuando complete el asistente de inicio rápido, realice la detección de dispositivos manualmente.

### 2 Configurando futuros sondeos

Asegúrese de que [Sondeo de rangos IP](#) esté activado y que el calendario de sondeo cumpla con las necesidades de su organización. Al configurar el horario de sondeo, utilice las recomendaciones para la red de frecuencia de sondeo.

También puede habilitar [Sondeo de configuración cero](#) si su red incluye dispositivos IPv6.

Si los dispositivos conectados a una red están incluidos en un dominio, se recomienda utilizar [el sondeo del controlador de dominio](#).

### 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**. Si lo desea, puede configurar las reglas para automático [el traslado de estos dispositivos](#) al grupo **Dispositivos administrados**. También puede definir reglas de retención.

Si omite esta etapa y no configura ninguna regla, los nuevos dispositivos que se descubran se agregarán al grupo **Dispositivos no asignados** y se quedarán allí. 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.

## Resultados

Completar las etapas anteriores tiene los siguientes resultados:

- El Servidor de administración de Kaspersky Security Center Linux 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**).

## Sondeo de intervalos IP

Kaspersky Security Center Linux intenta realizar una resolución de nombres inversa para cada dirección IPv4 desde el rango especificado a un nombre de DNS usando solicitudes de DNS estándar. Cuando la operación es exitosa, el servidor envía al nombre recibido una ICMP ECHO REQUEST (el mismo tipo de solicitud que se utiliza en el comando ping). Si el dispositivo responde, la información se añade a la base de datos de Kaspersky Security Center Linux. La resolución de nombres inversa es necesaria para excluir dispositivos de red que pueden tener dirección IP, pero que no son ordenadores (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. Si esta zona no está configurada, el sondeo de subred IP no dará resultados.

Inicialmente, Kaspersky Security Center Linux 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 Linux incluye automáticamente la red 192.168.0.0/24 en la lista de direcciones del sondeo. Kaspersky Security Center Linux sondea todas las direcciones desde 192.168.0.1 hasta 192.168.0.254.

Si solo está activado el sondeo de rangos de IP, Kaspersky Security Center Linux detecta dispositivos solo con direcciones IPv4. Si su red incluye dispositivos IPv6, active el [Sondeo de configuración cero](#) de dispositivos

## 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 **Detección y despliegue** → **Detección** → **Rangos 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 días concretos de las 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 manera 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 Linux 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 Linux incluye automáticamente la red 192.168.0.0/24 en la lista de direcciones del sondeo. Kaspersky Security Center Linux 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 activa el [Sondeo de Zeroconf](#), Kaspersky Security Center Linux sondeará toda la red.

*Para agregar un nuevo intervalo IP:*

1. En el menú principal, vaya a **Detección y despliegue** → **Detección** → **Rangos IP**.
2. Para agregar un nuevo intervalo IP, haga clic en el botón **Añadir**.
3. En la ventana que se abre, defina los siguientes ajustes:

- **[Nombre del rango 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 rango 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 \(horas\)](#)** ⓘ

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 **Activar sondeos de rangos 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**. 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 **Detección y despliegue** → **Detección** → **Rangos 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 **Añadir**.
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 Zeroconf

Este tipo de sondeo solo es compatible con los puntos de distribución basados en Linux.

Kaspersky Security Center Linux puede sondear redes que tienen dispositivos con direcciones IPv6. En este caso, no se especifican los rangos de IP y Kaspersky Security Center Linux sondea toda la red mediante el uso de una [red de configuración cero](#) (denominada *Zeroconf*). Para comenzar a usar Zeroconf, debe instalar la utilidad avahi-browse en el dispositivo Linux que sondea las redes, ya sea el Servidor de administración o un punto de distribución.

*Para habilitar el sondeo de Zeroconf:*

1. En el menú principal, vaya a **Detección y despliegue** → **Detección** → **Rangos IP**.
2. Haga clic en el botón **Propiedades**.
3. En la ventana abierta, active el botón **Usar Zeroconf para sondear las redes IPv6**.

Después de esto, Kaspersky Security Center Linux empieza a sondear su red. En este caso, se ignoran los rangos de IP especificados.

## Sondeo del controlador de dominio

Kaspersky Security Center Linux admite el sondeo de un controlador de dominio Microsoft Active Directory y un controlador de dominio Samba. Para un controlador de dominio Samba, [se utiliza Samba 4 como controlador de dominio 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.

Le recomendamos utilizar el sondeo del controlador de dominio si todos los dispositivos conectados a una red son miembros de un dominio. Si algunos de los dispositivos conectados a una red no están incluidos en el dominio, el sondeo del controlador de dominio no los podrá detectar.

## Requisitos previos

Antes de sondear un controlador de dominio, asegúrese de que los siguientes protocolos estén activados:

- Capa de seguridad y autenticación simple (SASL)
- Protocolo ligero de acceso a directorios (LDAP)

Asegúrese de que los siguientes puertos estén disponibles en el dispositivo controlador de dominio:

- 389 para SASL
- 636 para TLS

## Sondeo del controlador de dominio mediante el Servidor de administración

*Para sondear un controlador de dominio mediante el Servidor de administración, siga estos pasos:*

1. En el menú principal, vaya a **Detección y despliegue** → **Detección** → **Controladores de dominio**.
2. Haga clic en **Configuración de sondeo**.  
Se abre la ventana **Configuración de sondeo del controlador de dominio**.
3. Seleccione la opción **Activar el sondeo de controladores de dominio**.
4. En **Sondear dominios específicos**, haga clic en **Añadir**, y luego especifique la dirección y las credenciales de usuario del controlador de dominio.
5. Si es necesario, en la ventana **Configuración de sondeo del controlador de dominio**, especifique la programación de sondeo. 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.

- **[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 días concretos de las 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 manera predeterminada.

Si cambia las cuentas de usuario en un grupo de seguridad del dominio, estos cambios se mostrarán en Kaspersky Security Center Linux 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 del controlador de dominio utilizando un punto de distribución

También puede sondear un controlador de dominio utilizando 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 Microsoft Active Directory.

No se admite el sondeo con un punto de distribución de Mac.

*Para configurar el sondeo del controlador de dominio utilizando el punto de distribución, siga estos pasos:*

1. [Abra las propiedades del punto de distribución](#).

2. Seleccione la sección **Sondeo del controlador de dominio**.

3. Seleccione la opción **Activar 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 **Añadir**, 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 todo el bosque de dominio**
- **Sondear dominios específicos**

5. Haga clic en el botón **Programar sondeo** para especificar las opciones de la programación de sondeo si es necesario.

El sondeo solo se inicia según la programación especificada. El inicio manual del sondeo no está disponible.

Después de que se complete el sondeo, la estructura del dominio se mostrará en la sección **Controladores de dominio**.

Si configura y activa [reglas de movimiento del dispositivo](#), los dispositivos recién descubiertos automáticamente se incluyen en el grupo de **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 detectadas se pueden utilizar para [la autenticación de dominio en Kaspersky Security Center Web Console](#).

## Autenticación y conexión a un controlador de dominio

En la conexión inicial al controlador de dominio, el Servidor de administración identifica el protocolo de conexión. Este protocolo se usa para todas las conexiones futuras al controlador de dominio.

La conexión inicial a un controlador de dominio procede de la siguiente manera:

1. El Servidor de administración intenta conectarse al controlador de dominio a través de TLS.  
De forma predeterminada, la verificación del certificado no es obligatoria. Establezca el indicador `KLNAG_LDAP_TLS_REQCERT` en 1 para aplicar la verificación del certificado.  
De forma predeterminada, se usa la ruta de acceso a la autoridad de certificación (CA), que depende del 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 TLS falla, el Servidor de administración intenta conectarse al controlador de dominio a través de SASL (DIGEST-MD5).
3. Si la conexión SASL (DIGEST-MD5) falla, el Servidor de administración utiliza la autenticación sencilla a través de una conexión TCP no cifrada para conectarse al controlador de dominio.

Puede usar la utilidad `klscflag` para configurar indicadores.

Ejecute el símbolo del sistema y luego cambie el directorio actual al directorio con la utilidad `klscflag`. La utilidad `klscflag` se encuentra en el directorio donde está instalado el Servidor de administración. La ruta de instalación predeterminada es `/opt/kaspersky/ksc64/sbin`.

Por ejemplo, el siguiente comando fuerza la verificación del certificado:

```
klscflag -fset -pv klserver -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

## Configuración de un controlador de dominio Samba

Kaspersky Security Center Linux es compatible con un controlador de dominio de Linux que se ejecuta únicamente en Samba 4.

Un controlador de dominio Samba es compatible con las mismas extensiones de esquema que un controlador de dominio Microsoft Active Directory. Puede activar 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 es una acción opcional.

Le recomendamos activar 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 Linux y el controlador de dominio Samba.

*Para activar la compatibilidad total de un controlador de dominio Samba con un controlador de dominio Microsoft Active Directory, siga estos pasos:*

1. Ejecute el siguiente comando para utilizar la extensión de esquema RFC2307:

```
samba-tool domain provision --use-rfc2307 --interactive
```

2. Active la actualización del esquema en un controlador de dominio Samba. Para ello, añada 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 esquema principal.

Si desea sondear un controlador de dominio Samba correctamente, debe especificar el nombre de `netbios` y los parámetros del grupo de `trabajo` en el archivo `/etc/samba/smb.conf`.

## 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 Linux 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 no existentes pueden aparecer en Kaspersky Security Center Web Console.

Para evitar que se guarde información sobre máquinas virtuales inexistentes, Kaspersky Security Center Linux 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 el menú principal, vaya a **Detección y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**.
2. En el menú contextual del paquete de instalación del Agente de red, seleccione **Propiedades**.  
Se abre la ventana **Propiedades**.
3. En la ventana **Propiedades**, seleccione la sección **Avanzado**.
4. En la sección **Avanzado**, seleccione la opción **Activar modo dinámico para VDI**.

El dispositivo en el que se instalará el Agente de red forma parte de VDI.

## 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. Vaya a **Activos (dispositivos)** → **Reglas de movimiento**.
2. Haga clic en **Añadir**.
3. En la pestaña **Condiciones de reglas**, seleccione la pestaña **Máquinas virtuales**.
4. Establezca la regla **Es una máquina virtual** en **Sí** y **Parte de la infraestructura de escritorio virtual** en **Sí**.
5. Haga clic en **Guardar**.

# Prácticas recomendadas para el despliegue

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

- Servidor de administración: El componente principal, diseñado para administrar los dispositivos de una organización y almacenar datos en un DBMS.
- Kaspersky Security Center Web Console: la herramienta básica para el administrador. Puede instalar Kaspersky Security Center Web Console en el mismo dispositivo donde está instalado el Servidor de administración o en uno diferente.
- 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 Linux 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 en el dispositivo del administrador
- Instalación del Agente de red y aplicación de seguridad en dispositivos de la empresa.

## Guía de protección

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

El Servidor de administración de Kaspersky Security Center Linux 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.

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

La Guía de protección 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
- Gestión de la protección del Servidor de administración
- Gestión de la protección de dispositivos cliente
- Configuración de la protección para aplicaciones administradas
- Mantenimiento del Servidor de administración

- Transferencia de información a aplicaciones de terceros

## Despliegue 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 Linux](#) y su [interacción entre sí](#), así como con [esquemas de tráfico de datos y uso de puertos](#).

Sobre la base de 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 Linux, 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](#).

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

Recomendamos encarecidamente no instalar el Servidor de administración en un controlador de dominio, un servidor de terminal 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 directivas de seguridad para cada nodo.

## Cuentas para instalar y ejecutar el Servidor de administración

Durante el [despliegue del Servidor de administración](#), es necesario crear dos cuentas sin privilegios. Los servicios que se incluyen en el Servidor de administración funcionarán con estas cuentas sin privilegios. A la hora de asignar derechos y permisos a las cuentas, límitese a lo justo y necesario. Evite incluir cuentas innecesarias en el grupo "kadmins".

También debe crear una cuenta de DBMS interna. El Servidor de administración utiliza esta cuenta de DBMS interna para acceder al DBMS seleccionado.

El [conjunto de cuentas requeridas y sus derechos](#) depende del tipo de DBMS seleccionado y el método de creación de la base de datos del Servidor de administración.

## Seguridad de 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 de TLS estricta

Recomendamos usar el protocolo TLS de la versión 1.2 y posteriores, y restringir o prohibir los algoritmos de cifrado no seguros.

Puede [configurar protocolos de cifrado](#) (TLS) utilizado por el Servidor de administración. Tenga en cuenta que, en el momento del lanzamiento de una versión del Servidor de administración, la configuración del protocolo de cifrado está establecida de forma predeterminada para garantizar una transferencia de datos segura.

### 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, otorgue 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 utilizada, así como proporcionar puertos cerrados en los firewalls.

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

De manera predeterminada, los usuarios pueden iniciar sesión en Kaspersky Security Center Linux desde cualquier dispositivo donde esté instalado Kaspersky Security Center Web Console. Puede [configurar que el Servidor de administración](#) únicamente acepte conexiones de dispositivos que tengan una dirección IP permitida.

## Cuentas y autenticación

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

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

Cuando la verificación en dos pasos está activada para su propia cuenta, cada vez que inicie sesión en Kaspersky Security Center Web Console, debe introducir su nombre de usuario, contraseña y un código de seguridad adicional de un solo uso. Para recibir un código de seguridad de un solo uso, debe instalar una aplicación de autenticación en su equipo 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 aplicación de autenticación en el mismo dispositivo desde el que se establece la conexión con el Servidor de administración. Puede instalar una aplicación de autenticación en su dispositivo móvil.

### Uso de la autenticación de dos factores para un sistema operativo

Recomendamos utilizar la autenticación multifactor (MFA) para la autenticación en el dispositivo Servidor de administración mediante un token, una tarjeta inteligente u otro método (si es posible).

### Prohibición de guardar la contraseña de administrador

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 16 caracteres
- La contraseña debe contener 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 Linux 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.

## 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.

## Restricción de la asignación de la función de Administrador principal

Al usuario creado por la utilidad kladduser se le asigna la función de Administrador principal en la lista de control de acceso (ACL) del Servidor de administración. Recomendamos evitar la asignación de la función de Administrador principal a un gran número de usuarios.

## Configuración de 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 Linux 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:

- Gestión de 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 Servidor de administración cuando ocurre 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 separada para la instalación remota de aplicaciones. Puede [asignar un rol](#) o [permisos](#) a la cuenta separada.

## Auditoría periódica de todos los usuarios

Recomendamos realizar una auditoría periódica 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.

## Gestión de la protección del Servidor de administración

### Selección de un software de protección del Servidor de administración

Según el tipo de despliegue del Servidor de administración y la estrategia de protección general, seleccione la aplicación para proteger el dispositivo del Servidor de administración.

Si implementa 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 Cyber Security for Nodes. Recomendamos instalar esta aplicación en dispositivos que estén incluidos en una red industrial. Kaspersky Industrial Cyber Security for Nodes es una aplicación que cuenta con certificados de compatibilidad con varios fabricantes de software industrial.
- Productos de seguridad recomendados. Si el Servidor de administración está instalado en un dispositivo con otro software, recomendamos tener en cuenta las recomendaciones de ese proveedor de software sobre la compatibilidad de los productos de seguridad (puede que ya haya recomendaciones para seleccionar una solución de seguridad, y quizá 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 directiva 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 Kaspersky Security Center Web Console.

De manera predeterminada, el [Servidor de administración utiliza el puerto 13299](#) para recibir conexiones desde 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 este puerto.

## Gestión de la protección de dispositivos cliente

### Restricción de 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 añade una clave de licencia a un paquete de instalación, todos los usuarios con derechos de lectura en esta carpeta podrán acceder a dicha clave (directamente o mediante el [servidor web](#) integrado en el Servidor de administración).

Para evitar comprometer 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 añadir clave de licencia a una aplicación administrada, y añadir un código de activación o un archivo clave manualmente 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 las directivas. Estas configuraciones de directivas pueden no ser deseables para su distribución a dispositivos invitados y que no sean de confianza.

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 que tengan instalado el Agente de red 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 evite asignar puntos de distribución automáticamente, ya que, por ejemplo, la información privada de las cuentas utilizadas para forzar las tareas de instalación remota puede transferirse a puntos de distribución por medio del sistema operativo.

Para redes industriales y redes pequeñas, puede [asignar manualmente dispositivos para que actúen como puntos de distribución](#).

También puede ver el [Informe sobre la actividad de los puntos de distribución](#).

## Configuración de la protección para aplicaciones administradas

### Directivas para aplicaciones administradas

Recomendamos crear una [directiva](#) para cada tipo de aplicaciones y componentes de Kaspersky Security Center Linux (Agente de red, Kaspersky Endpoint Security para Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Agent y otros) que se utiliza. Esta directiva debe aplicarse a todos los dispositivos administrados (el grupo de administración raíz) o a un grupo independientes al que se mueven automáticamente los nuevos dispositivos administrados de acuerdo con las reglas de movimiento configuradas.

### Especificación de la contraseña para desactivar la protección y desinstalar la aplicación

**Recomendamos encarecidamente activar la protección con contraseña para evitar que los intrusos desactiven o desinstalen las aplicaciones de seguridad de Kaspersky.** En las plataformas donde se admite la protección con contraseña, puede establecer la contraseña, por ejemplo, para Kaspersky Endpoint Security, el [Agente de red](#) y otras aplicaciones de Kaspersky. Después de activar la protección con contraseña, recomendamos bloquear la configuración correspondiente al cerrar 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 activar 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 de eliminación de Kaspersky Security Center Web Console (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, si el uso de servicios en la nube está prohibido por ley u otras normativas, puede desactivar 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 controladores del dominio 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.

## 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 para 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:

- Comprueba la base de datos en busca de errores
- 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

Recomendamos encarecidamente 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 una respuesta oportuna a los problemas de seguridad, recomendamos configurar las [funciones de supervisión e informes](#).



## Exportación de eventos a sistemas SIEM

Para la detección rápida de problemas de seguridad antes de que se produzcan daños importantes, recomendamos utilizar [la exportación de eventos en un sistema SIEM](#).

## Notificaciones por correo electrónico de eventos de auditoría

Kaspersky Security Center Linux le permite recibir información sobre los eventos que ocurren durante el 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 tengan lugar un pequeño número, algo que resulta muy aplicable al correo.

## Preparativos para el despliegue

Esta sección describe los pasos que debe completar antes de realizar el despliegue de Kaspersky Security Center Linux.

## Planificación del despliegue de Kaspersky Security Center Linux

Esta sección proporciona la información sobre las opciones más convenientes para el despliegue de los componentes de Kaspersky Security Center Linux 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 de 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:

- Despliegue de un sistema de protección 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.

- 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 no admite el despliegue a través de las directivas de grupo de Microsoft Active Directory®.

## Acerca de la planificación del despliegue de Kaspersky Security Center Linux en la red de una organización

Un Servidor de administración puede admitir un máximo de 20 000 dispositivos (con el servidor MariaDB como DBMS). Cuando el número total de dispositivos en la red de una organización supera los 20 000, 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 Linux](#)" proporciona descripciones detalladas de las configuraciones estándares de Kaspersky Security Center Linux. 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
- 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 de 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 Linux

Esta sección describe las configuraciones estándares siguientes usadas para la distribución de componentes de Kaspersky Security Center Linux 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 hasta 20 000 dispositivos (con el servidor MariaDB como DBMS). Considere 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 (ordenadores portátiles), cree perfiles de conexión del Agente de red en la directiva del Agente de red. Tenga en cuenta que los perfiles de conexión del Agente de red solo son compatibles con los dispositivos de 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 detalles: [Habilitación de un servidor push](#).

## Selección de un DBMS

La siguiente tabla enumera las opciones de DBMS válidas, así como las recomendaciones y restricciones sobre su uso.

Recomendaciones y restricciones en DBMS

| DBMS                                                                   | Recomendaciones y restricciones                                                                            |
|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| MySQL ( <a href="#">ver versiones compatibles</a> )                    | Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 20 000 dispositivos. |
| MariaDB ( <a href="#">ver versiones compatibles</a> )                  | Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 20 000 dispositivos. |
| PostgreSQL, Postgres Pro ( <a href="#">ver versiones compatibles</a> ) | Utilice este DBMS si planea ejecutar un solo Servidor de administración para menos de 50 000 dispositivos. |

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

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](#).

Si decide instalar PostgreSQL o Postgres Pro DBMS, asegúrese de haber especificado 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.

Si instala [MariaDB](#), [PostgreSQL](#), o [Postgres Pro](#), use la configuración recomendada para garantizar que el DBMS funcione correctamente.

## 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 correcciones recomendadas para vulnerabilidades en el software de Microsoft. Los especialistas de Kaspersky crean y actualizan periódicamente la lista.
- Reparar vulnerabilidades en software de terceros que no sea el software de 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.

Tenga en cuenta que Kaspersky Security Center Linux no admite el despliegue con directivas de grupo de Microsoft Windows.

Puede utilizar puntos de distribución ubicados en 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 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 puerta de enlace de conexión en 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 **Añadir 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 ordenadores 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** → **Conectar con el Servidor de administración usando 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 ordenadores 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 distribuir actualizaciones, que se pueden recuperar desde el Servidor de administración o desde los servidores de Kaspersky. En este último caso, [configure la descarga de actualizaciones para un punto de distribución](#).

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.

## 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.

## 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.

## Configuración de la red para interactuar con servicios externos

Kaspersky Security Center Linux utiliza la siguiente configuración de red para interactuar con los servicios externos.

### Configuración de red

| Configuración de red               | Dirección                                                                                                                                                                                                                                                            | Descripción                                                                                             |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Puerto: 443<br>Protocolo:<br>HTTPS | activation-<br>v2.kaspersky.com/activation-service/activation-service.svc                                                                                                                                                                                            | Activación de la aplicación.                                                                            |
| Puerto: 443<br>Protocolo:<br>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 | <a href="#">Actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky.</a> |

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                               | <p>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</p>                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <p>Puerto: 443<br/> Protocolo:<br/> HTTPS</p> | <p>https://downloads.upd.kaspersky.com</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>• <a href="#">Actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky.</a></li> <li>• 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 Linux comprueba si se puede acceder a los servidores de Kaspersky. Si no es posible acceder a los servidores mediante el DNS del sistema, la aplicación utiliza <a href="#">servidores de DNS públicos.</a></li> </ul> |
| <p>Puerto: 80<br/> Protocolo:<br/> HTTP</p>   | <p>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</p> | <p><a href="#">Actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky.</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                   |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
|                                                  | <p>http://p14.upd.kaspersky.com</p> <p>http://p15.upd.kaspersky.com</p> <p>http://p16.upd.kaspersky.com</p> <p>http://p17.upd.kaspersky.com</p> <p>http://p18.upd.kaspersky.com</p> <p>http://p19.upd.kaspersky.com</p> <p>http://downloads0.kaspersky-labs.com</p> <p>http://downloads1.kaspersky-labs.com</p> <p>http://downloads2.kaspersky-labs.com</p> <p>http://downloads3.kaspersky-labs.com</p> <p>http://downloads4.kaspersky-labs.com</p> <p>http://downloads5.kaspersky-labs.com</p> <p>http://downloads6.kaspersky-labs.com</p> <p>http://downloads7.kaspersky-labs.com</p> <p>http://downloads8.kaspersky-labs.com</p> <p>http://downloads9.kaspersky-labs.com</p> <p>http://downloads.kaspersky-labs.com</p> <p>http://cm.k.kaspersky-labs.com</p> |                                                   |
| <p>Puerto: 443</p> <p>Protocolo: HTTPS</p>       | ds.kaspersky.com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Usar <a href="#">Kaspersky Security Network</a> . |
| <p>Puerto: 443, 1443</p> <p>Protocolo: HTTPS</p> | <p>ksn-a-stat-geo.kaspersky-labs.com</p> <p>ksn-file-geo.kaspersky-labs.com</p> <p>ksn-verdict-geo.kaspersky-labs.com</p> <p>ksn-url-geo.kaspersky-labs.com</p> <p>ksn-a-p2p-geo.kaspersky-labs.com</p> <p>ksn-info-geo.kaspersky-labs.com</p> <p>ksn-cinfo-geo.kaspersky-labs.com</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Usar <a href="#">Kaspersky Security Network</a> . |
| <p>Protocolo: HTTPS</p>                          | <p>click.kaspersky.com</p> <p>redirect.kaspersky.com</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Seguir los enlaces desde la interfaz.             |
| <p>Puerto: 80</p> <p>Protocolo: HTTP</p>         | <p>http://crl.kaspersky.com</p> <p>http://ocsp.kaspersky.com</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Infraestructura de clave pública (PKI).           |
| <p>Puerto: 443</p> <p>Protocolo: HTTPS</p>       | https://ipm-klca.kaspersky.com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <a href="#">Anuncios de marketing</a> .           |

Para una interacción adecuada de Kaspersky Security Center Linux 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 MITM](#)).

Para descargar las actualizaciones a través del protocolo HTTP o HTTPS utilizando la utilidad `klscflag`, siga estos pasos:

1. Ejecute el símbolo del sistema y luego cambie el directorio actual al directorio con la utilidad `klscflag`. La utilidad `klscflag` se encuentra en el directorio donde está instalado el Servidor de administración. La ruta de instalación predeterminada es `/opt/kaspersky/ksc64/sbin`.
2. Si desea descargar [actualizaciones](#) a través del protocolo HTTP, ejecute uno de los siguientes comandos en la cuenta raíz:

- En el dispositivo en el que se encuentra instalado el Servidor de administración:  

```
klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
```
- En un punto de distribución:  

```
klscflag -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 la cuenta raíz:

- En el dispositivo en el que se encuentra instalado el Servidor de administración:  

```
klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
```
- En un punto de distribución:  

```
klscflag -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 Linux distribuido en dispositivos corporativos normalmente comienza con la instalación del Agente de red en ellos.

En Microsoft Windows XP, es posible que el Agente de red no realice las siguientes operaciones correctamente: descargar actualizaciones directamente desde los servidores de Kaspersky (como punto de distribución) y funcionar como servidor proxy de KSN (como punto de distribución).

## 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.
- 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 Linux 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 Linux.
- En el modo forzado, usando opciones especiales en la tarea de instalación remota de Kaspersky Security Center Linux.
- Al enviar vínculos de usuarios del dispositivo a paquetes independientes generados por Kaspersky Security Center Linux. 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 además de Microsoft Windows, la configuración inicial del Agente de red en dispositivos administrados se debe realizar a través de herramientas de terceros disponibles. 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 [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 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 capacidad de los canales de la red en esas subredes.
- 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, 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 Linux como con la mayor parte de herramientas de terceros. Este método consiste en crear paquetes de instalación de aplicaciones en Kaspersky Security Center Linux.

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 Kaspersky Security Center Web Console, durante la creación del paquete de instalación. Al realizar la instalación remota de aplicaciones a través de herramientas de Kaspersky Security Center Linux, 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 Linux en una subcarpeta dedicada [de la carpeta compartida](#).

No especifique ningún detalle de cuentas privilegiadas en los parámetros de los paquetes de instalación.

No se admite el despliegue mediante directivas de grupo de Microsoft Windows.

Inmediatamente después de la instalación de Kaspersky Security Center Linux, 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.

## Acerca de las tareas de instalación remota en Kaspersky Security Center Linux

Kaspersky Security Center Linux 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). Puede crear una tarea de instalación remota tanto para un grupo de administración determinado como para dispositivos específicos o una selección de dispositivos (estas tareas se muestran en Kaspersky Security Center Web Console, 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 supervisión de resultados.

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 Linux.

Para capturar e instalar imágenes de disco, use las herramientas de terceros disponibles en la organización.



## 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:

- 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 la red con paquetes de instalación independientes desde un dispositivo.

## 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 Kaspersky Security Center Web Console como un solo dispositivo. Este problema se produce porque la clonación hace que los nuevos dispositivos conserven datos internos idénticos, lo que permite al Servidor de administración asociar un dispositivo con su propio registro en Kaspersky Security Center Web Console.

El *modo de clonación de disco del Agente de red* especial le permite evitar la visualización incorrecta de dispositivos nuevos en Kaspersky Security Center Web Console después 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 registro en Kaspersky Security Center Web Console. Después de completar la clonación de la imagen del dispositivo de referencia, los dispositivos nuevos se muestran en Kaspersky Security Center Web Console correctamente (con registros 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 `klmagchk`.
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, escriba 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, escriba 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, escriba el siguiente comando en la línea de comandos de la utilidad: `klmover -cloningmode 0`.

## Despliegue forzado con la tarea de instalación remota de Kaspersky Security Center Linux

Si tiene que empezar a distribuir los Agentes de red u otras aplicaciones inmediatamente, sin esperar la próxima vez que los dispositivos de destino inicien sesión en el dominio, o si algún dispositivo de destino que no sea miembro del dominio de Active Directory está disponible, puede forzar la instalación de paquetes de instalación seleccionados a través de la tarea de instalación remota de Kaspersky Security Center Linux.

En este caso, puede especificar dispositivos de destino explícitamente (con una lista), o al seleccionar el grupo de administración de Kaspersky Security Center Linux al cual pertenecen, o al crear una selección de dispositivos basados en 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.

Este tipo de instalación consiste en la copia de archivos al recurso administrativo (admin\$) en cada dispositivo y la realización del registro remoto de los servicios compatibles en ellos. Solo los puntos de distribución designados pueden realizar un despliegue forzado en dispositivos Windows desde el recurso administrativo. Las condiciones siguientes se deben cumplir en este caso:

- Los dispositivos deben estar disponibles para la conexión desde el Servidor de administración o desde el lado del punto de distribución.
- La resolución del nombre para dispositivos de destino debe funcionar correctamente en la red.
- Las carpetas compartidas administrativas (admin\$) deben permanecer habilitadas en dispositivos de destino.
- El servicio del sistema del Servidor se debe ejecutar en dispositivos de destino (de forma predeterminada, se está ejecutando).
- Los puertos siguientes se deben abrir en los dispositivos de destino para permitir el acceso remoto a través de herramientas de Windows: TCP 139, TCP 445, UDP 137 y UDP 138.
- El modo simple de uso compartido de archivos se debe deshabilitar en los dispositivos de destino.
- En los dispositivos de destino, la carpeta compartida de acceso y el modelo de seguridad deben estar configurados como *Clásico: los usuarios locales se autentican como ellos mismos*, pero de ningún modo pueden estar configurados como *Invitado únicamente: los usuarios locales se autentican como invitados*.
- Los dispositivos de destino deben ser miembros del dominio, o las cuentas uniformes con derechos del administrador se deben crear en los dispositivos de destino de antemano.

Los dispositivos en grupos de trabajo se pueden ajustar de acuerdo con los requisitos indicados anteriormente usando la utilidad riprep.exe, que se describe [en el sitio web del Servicio de soporte técnico de Kaspersky](#).

Durante la instalación en dispositivos nuevos que todavía no se han asignado a ninguno de los grupos de administración de Kaspersky Security Center Linux, 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.

La instalación automática es una manera simplificada de crear tareas para la instalación forzada de aplicaciones. Para hacer esto, 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.

La instalación forzada también se puede aplicar 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. Para hacer la instalación forzada posible, debe proporcionar puntos de distribución a cada una de las redes aisladas.

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. Sin embargo, 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 que seleccione dispositivos potentes, con unidades de almacenamiento de alto rendimiento como puntos de distribución. Además, el espacio libre del disco en la partición con la carpeta `/var/opt/kaspersky/klnagent_srv/` 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 Linux

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 Linux, 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 Linux.

Puede usar Kaspersky Security Center Linux 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 Linux. 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.

## 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 **Usando 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 el 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 los paquetes de instalación a los dispositivos de destino a través de los 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 caché en la carpeta `/var/opt/kaspersky/klnagent_srv/1093/.working/`. 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 eliminan, los datos correspondientes automáticamente se eliminarán de la carpeta FTServer.

Los datos recibidos por los puntos de distribución se guardan en la carpeta `/var/opt/kaspersky/klnagent_srv/1103/`.

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 Kaspersky Security Center Web Console. La modificación de la configuración de un paquete de instalación en Kaspersky Security Center Web Console hace que el Servidor de administración actualice la imagen del paquete en la 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 Linux, 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 (cierres o reinicios).
- **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.

## Supervisión del despliegue

Para supervisar el despliegue de Kaspersky Security Center Linux y asegurarse de que una aplicación de seguridad y un Agente de red estén instalados en los dispositivos administrados, [utilice la función de supervisión e informes](#):

- Utilice el widget de despliegue del [panel](#) para supervisar el despliegue en tiempo real.
- Utilice [informes](#) para obtener información detallada.

## Configuración de instaladores

Esta sección proporciona la información sobre los archivos de instaladores de Kaspersky Security Center Linux 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 Linux para dispositivos Windows utilizan 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)

El instalador del Agente de red tiene la función de trabajar con el archivo de respuesta (ss\_install.xml), donde se integran los parámetros para la instalación en el modo silencioso sin la participación del usuario. 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 Linux 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 Linux. 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 Linux, al modificar la parámetros de los paquetes de instalación en Kaspersky Security Center Web Console.

## 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

La siguiente tabla describe las propiedades que puede configurar al instalar Kaspersky Security Center Linux en modo silencioso.

Parámetros de instalación del Servidor de administración en modo no interactivo

| Nombre de la variable     | Obligatoria | Descripción                                                                            | Valores po      |
|---------------------------|-------------|----------------------------------------------------------------------------------------|-----------------|
| EULA_ACCEPTED             | Sí          | Confirme que entiende y acepta los términos del Contrato de licencia de usuario final. | 1               |
| PP_ACCEPTED               | Sí          | Confirme que entiende y acepta los términos de la Política de privacidad.              | 1               |
| KLSRV_UNATT_SERVERADDRESS | Sí          | El nombre DNS o la dirección IP estática del Servidor de administración.               | Nombre DNS o IP |
| KLSRV_UNATT_PORT_SRV      | No          | El número de puerto del                                                                | Número de pue   |

|                           |    |                                                                                                                                                                                          |                                                                                                          |
|---------------------------|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
|                           |    | Servidor de administración. Opcional. El valor predeterminado es 14000.                                                                                                                  |                                                                                                          |
| KLSRV_UNATT_PORT_SRV_SSL  | No | El número de puerto SSL del Servidor de administración. Opcional. El valor predeterminado es 13000.                                                                                      | Número de pue                                                                                            |
| KLSRV_UNATT_PORT_KLOAPI   | No | El número de puerto KLOAPI del Servidor de administración. Opcional. El valor predeterminado es 13299.                                                                                   | Número de pue                                                                                            |
| KLSRV_UNATT_PORT_GUI      | No | El número de puerto de la GUI del Servidor de administración. Opcional. El valor predeterminado es 13291.                                                                                | Número de pue                                                                                            |
| KLSRV_UNATT_NETRANGETYPE  | No | El número aproximado de dispositivos que desea administrar. Opcional. El valor predeterminado es 1.                                                                                      | 1 para 1 a 100 d<br>en red.<br>2 para 101 a 10C<br>dispositivos en<br>3 para más de 1<br>dispositivos en |
| KLSRV_UNATT_DBMS_TYPE     | Sí | El tipo de sistema de administración de bases de datos: MySQL (MariaDB) o Postgres.                                                                                                      | mysql<br>o<br>postgres                                                                                   |
| KLSRV_UNATT_DBMS_INSTANCE | Sí | La dirección IP del servidor de la base de datos.                                                                                                                                        | Dirección IP                                                                                             |
| KLSRV_UNATT_DBMS_PORT     | Sí | El puerto del servidor de la base de datos. El valor predeterminado para MySQL (MariaDB) es 3306; el valor predeterminado para Postgres es 5432.                                         | 3306<br>o<br>5432                                                                                        |
| KLSRV_UNATT_DB_NAME       | Sí | El nombre de la base de datos.                                                                                                                                                           | kav                                                                                                      |
| KLSRV_UNATT_DBMS_LOGIN    | Sí | El nombre de usuario de un usuario que tiene acceso a la base de datos.                                                                                                                  |                                                                                                          |
| KLSRV_UNATT_DBMS_PASSWORD | Sí | La contraseña de un usuario que tiene acceso a la base de datos.                                                                                                                         |                                                                                                          |
| KLSRV_UNATT_KLADMINSGROUP | Sí | El nombre del grupo de seguridad para los servicios.                                                                                                                                     | kladmins                                                                                                 |
| KLSRV_UNATT_KLSRVUSER     | Sí | El nombre de la cuenta para iniciar el servicio del Servidor de administración. La cuenta debe ser miembro del grupo de seguridad especificado en la variable KLSRV_UNATT_KLADMINSGROUP. | ksc                                                                                                      |
| KLSRV_UNATT_KLSVCUSER     | Sí | El nombre de la cuenta para iniciar otros servicios. La cuenta debe ser miembro del grupo de                                                                                             | ksc                                                                                                      |



|                                                                                                                                                                                                                        |                                    |                                                                     |                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|---------------------------------------------------------------------|-------------------------------------|
|                                                                                                                                                                                                                        |                                    | seguridad especificado en la variable<br>KLSRV_UNATT_KLADMINSGROUP. |                                     |
| Si el Servidor de administración se despliega como un <a href="#">clúster de conmutación por error de Kaspersky Security Center Linux</a> , el archivo de respuesta debe incluir las siguientes variables adicionales: |                                    |                                                                     |                                     |
| KLFOC_UNATT_NODE                                                                                                                                                                                                       | Sí                                 | El número de nodo (1 o 2).                                          | 1<br>0<br>2                         |
| KLFOC_UNATT_STATE_SHARE_MOUNT_PATH                                                                                                                                                                                     | Sí                                 | El punto de montaje de la carpeta compartida de estados.            |                                     |
| KLFOC_UNATT_DATA_SHARE_MOUNT_PATH                                                                                                                                                                                      | Sí                                 | El punto de montaje de la carpeta compartida de datos.              |                                     |
| KLFOC_UNATT_CONN_MODE                                                                                                                                                                                                  | Sí                                 | El modo de conectividad del clúster de conmutación por error.       | VirtualAdapter<br>o<br>ExternalLoad |
| En caso de que la variable KLFOC_UNATT_CONN_MODE tenga el valor VirtualAdapter, el archivo de respuesta de las siguientes variables adicionales:                                                                       |                                    |                                                                     |                                     |
| KLFOC_UNATT_CONN_MODE_VA_NAME                                                                                                                                                                                          |                                    | El nombre del adaptador de red virtual.                             |                                     |
| KLFOC_UNATT_CONN_MODE_VA_IPV4                                                                                                                                                                                          | Se requiere una de estas variables | La dirección IP del adaptador de red virtual.                       | Dirección IP                        |
| KLFOC_UNATT_CONN_MODE_VA_IPV6                                                                                                                                                                                          |                                    | La dirección IPv6 del adaptador de red virtual.                     | Dirección IPv6                      |

## 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 | <ul style="list-style-type: none"> <li>1: he leído, comprendo y acepto en su totalidad los términos del <a href="#">Contrato de licencia de usuario final</a>.</li> <li>0: No acepto los términos del Contrato de licencia (no se realiza la instalación).</li> <li>Sin valor: no acepto los términos del Contrato de</li> </ul> |

|                                           |                                                                                                                                                                        |                                                                                                                                                              |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           |                                                                                                                                                                        | licencia (no se realiza la instalación).                                                                                                                     |
| DONT_USE_ANSWER_FILE                      | Lea la configuración de instalación desde el archivo de respuesta                                                                                                      | <ul style="list-style-type: none"> <li>• 1—No usar.</li> <li>• Otro valor o ningún valor—Leer.</li> </ul>                                                    |
| 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                                                                                                                                             | <ul style="list-style-type: none"> <li>• 1: Usar</li> <li>• Otro valor o ningún valor: No usar</li> </ul>                                                    |
| OPENUDP                                   | Abrir un puerto UDP o no                                                                                                                                               | <ul style="list-style-type: none"> <li>• 1: Abrir</li> <li>• Otro valor o ningún valor: No abrir</li> </ul>                                                  |
| UDP                                       | Número de puerto UDP                                                                                                                                                   | Valor numérico.                                                                                                                                              |
| USEPROXY                                  | Usar un servidor proxy o no                                                                                                                                            | <ul style="list-style-type: none"> <li>• 1: Usar</li> <li>• Otro valor o ningún valor: No usar</li> </ul>                                                    |
| PROXYLOCATION<br>(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                                                                                                                         | <ul style="list-style-type: none"> <li>• 0: No usar la puerta de enlace de conexión</li> <li>• 1: Use este Agente de red como puerta de enlace de</li> </ul> |

|                |                                                                                                     |                                                                                                                                                                                                                                                                        |
|----------------|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |                                                                                                     | <p>conexión</p> <ul style="list-style-type: none"> <li>• 2: Conectarse al Servidor de administración mediante una puerta de enlace de conexión</li> </ul>                                                                                                              |
| GATEWAYADDRESS | Dirección de la puerta de enlace de conexión                                                        | Valor de cadena.                                                                                                                                                                                                                                                       |
| CERTSELECTION  | Método de recibir un certificado                                                                    | <ul style="list-style-type: none"> <li>• GetOnFirstConnection; Reciba un certificado del Servidor de administración</li> <li>• GetExistent: Seleccionar un certificado existente. Si se selecciona esta opción, se deberá especificar la propiedad CERTFILE</li> </ul> |
| CERTFILE       | Ruta al archivo de certificado                                                                      | Valor de cadena.                                                                                                                                                                                                                                                       |
| VMVDI          | Habilitar el modo dinámico para la Infraestructura de escritorio virtual (VDI)                      | <ul style="list-style-type: none"> <li>• 1: Habilitar.</li> <li>• 0: No habilitar.</li> <li>• Sin valor: No habilitar.</li> </ul>                                                                                                                                      |
| LAUNCHPROGRAM  | Ejecutar el inicio del servicio del Agente de red después de la instalación                         | <ul style="list-style-type: none"> <li>• 1: Iniciar.</li> <li>• Otro valor o ningún valor: No iniciar.</li> </ul>                                                                                                                                                      |
| 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 Linux 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 Linux 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 desactivación de algunas funciones de Kaspersky Security Center Linux 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 del 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 Kaspersky Security Center Web Console.

## Compatibilidad con máquinas virtuales dinámicas

Kaspersky Security Center Linux 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 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 Linux en la red de la organización, se añadirá 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 **Activar modo dinámico para VDI**:

- Para 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 **Activar 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 eventos tras la eliminación de los dispositivos** y especifique el plazo de almacenamiento máximo para los eventos (en días).

## 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 **Activar 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 Linux 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 Linux.

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 Linux. 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 ha añadido a Kaspersky Security Center Linux 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 Linux.

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 kbackup.

## 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 Linux también admite la opción de instalación local de las aplicaciones que usan un paquete de instalación independiente. Kaspersky Security Center Linux 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. 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 enlace **Solo instalación Agente de red de Kaspersky Security Center 15** para iniciar el asistente de instalación del Agente de red. Siga las instrucciones del asistente.

Mientras se ejecuta el Asistente de instalación, puede especificar la configuración avanzada del Agente de red (consulte a continuación).

3. Si quiere utilizar el dispositivo como la puerta de enlace de conexión de un grupo de administración específico, en la ventana **Puerta de enlace de conexión** del asistente de instalación, seleccione **Usar el Agente de red como puerta de enlace de conexión en DMZ**.

4. Para configurar el Agente de red durante la instalación en una máquina virtual:

a. Si planea crear máquinas virtuales dinámicas desde la imagen de la máquina virtual, active el modo dinámico del Agente de red para la infraestructura de escritorio virtual (VDI). Para ello, en la ventana **Configuración avanzada** del Asistente de instalación, seleccione la opción **Activar modo dinámico para VDI**.

Omita este paso si no va a crear máquinas virtuales dinámicas a partir de la imagen de la máquina virtual.

b. Optimice la operación del Agente de red para VDI. Para ello, en la ventana **Configuración avanzada** del asistente de instalación, seleccione la opción **Optimizar la configuración para VDI**.

Se desactivará el análisis de los archivos ejecutables para buscar vulnerabilidades al iniciarse el dispositivo. Además, esto deshabilita el envío de información sobre los objetos siguientes al Servidor de administración:

- Registro de hardware
- Aplicaciones instaladas en el dispositivo
- Actualizaciones de Microsoft Windows que se deben instalar en el dispositivo cliente local
- Vulnerabilidades de software detectadas en el dispositivo cliente local

Además, podrá habilitar el envío de esta información en las propiedades del Agente de red o en la configuración de la directiva del Agente de red.

Cuando el asistente de instalación se haya completado, el Agente de red estará instalado en el dispositivo.

Puede ver las propiedades del servicio del Agente de red; también puede iniciar, detener y supervisar la actividad del Agente de red mediante las herramientas estándar de Microsoft Windows: 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 Linux, en la carpeta Packages\NetAgent\exec.

*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 >
```

en el que `setup_parameters` es una lista de parámetros de configuración y sus respectivos valores separados por espacios (`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 11 y versiones posteriores, 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 puertos 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](#).

## 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 Linux. La instalación se facilita con el asistente y no requiere la 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 Linux. 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.

*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 para crear paquete de instalación independiente. Siga las instrucciones del asistente.

En el paso final del asistente, seleccione un método para transmitir 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 manera 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 manera 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 manera predeterminada.

- [Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir](#) ⓘ

Si esta opción está activada, todas las actualizaciones y parches descargados para el Servidor de administración, el Agente de red, Kaspersky Security Center Web Console, el Servidor de dispositivos móviles de Exchange 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 habilitada de manera 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.

- [Utilizar certificado de 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.

- [Utilizar 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 manera 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 habilitada de manera 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 puertos del Agente de red en el Firewall de Microsoft Windows](#)

Cuando se habilita esta opción, se agregan los puertos UDP que el Agente de red necesita para funcionar a la lista de exclusiones del Firewall de Microsoft Windows.

Esta opción está habilitada de manera predeterminada.

## 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:

- [Activar 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 manera 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 manera 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 activada, 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 está desactivada, 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               | ✓       | ✓<br>(excepto las opciones <b>Abrir puertos del Agente de red en el Firewall de Microsoft Windows</b> y <b>Utilizar solo detección automática de servidor proxy</b> ) | ✓<br>(excepto las opciones <b>Abrir puertos del Agente de red en el Firewall de Microsoft Windows</b> y <b>Utilizar solo detección automática de servidor proxy</b> ) |

|                         |   |                                               |                                               |
|-------------------------|---|-----------------------------------------------|-----------------------------------------------|
| Avanzado                | ✓ | ✓                                             | ✓                                             |
| Componentes adicionales | ✓ | ✓                                             | ✓                                             |
| Etiquetas               | ✓ | (excepto las reglas de etiquetado automático) | (excepto las reglas de etiquetado automático) |
| Historial de revisiones | ✓ | ✓                                             | ✓                                             |

## 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. Si la programación especificada automáticamente de la tarea de análisis de grupo no es apropiada para su organización, debe configurar de forma manual la programación más conveniente para esta tarea según las reglas del lugar de trabajo adoptadas en la organización.

Por ejemplo, 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. En este caso, debe configurar la tarea de análisis de grupo manualmente.

## Administración de dispositivos cliente

En esta sección, se describe cómo administrar los dispositivos incluidos en los 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.

- **[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**.

- **[Nombre de grupo completo](#)**

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 Linux.

- [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](#)

Grupo de trabajo que contiene el dispositivo.

- [Nombre DNS](#)

Nombre del dominio DNS del dispositivo cliente.

- [Nombre NetBIOS](#)

Nombre del dispositivo cliente.

- **Dirección IPv6**

- La sección **Sistema** proporciona información sobre el sistema operativo instalado en el dispositivo cliente:

- **Sistema operativo**

- **Arquitectura de 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 la 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 detectado](#)

Número total de amenazas detectadas en el dispositivo cliente desde la instalación de la aplicación antivirus (primer análisis del dispositivo) o desde la última vez que el contador de amenazas se puso en cero.

- [Objetos que no se han podido desinfectar](#)

Número de archivos no procesados en el dispositivo cliente.

Este campo no refleja el número de archivos no procesados en dispositivos móviles.

- [Estado del 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](#).

Los archivos solo se pueden cifrar en los dispositivos administrados en los que está instalado 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 del dispositivo puede ser diferente al definido por Kaspersky Security Center Linux Cloud Console.

- [Aplicaciones](#)

Esta pestaña enumera todas las aplicaciones de Kaspersky instaladas en el dispositivo cliente. Haga 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.

- [Perfiles de directiva y directivas activas](#)

Esta pestaña enumera las directivas y los perfiles de directivas que están activos en el dispositivo administrado.

- [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 no se puede establecer una conexión, no se mostrará ningún estado.

- [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 pueden ser creados 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) e incluir 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 los 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 es definido por la aplicación de Kaspersky que crea el problema de seguridad. Si desea resaltar los problemas de seguridad procesados de la lista, active 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.

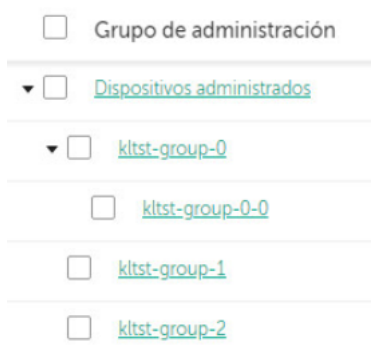
- [Propiedades](#) ?

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.
- **Diagnósticos remotos.** En esta sección, puede realizar un [diagnóstico remoto de dispositivos cliente](#).

## 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 y máquinas virtuales, al grupo **Dispositivos administrados** y añadir grupos anidados (ver la figura de abajo).



*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 **Añadir**.
4. En la ventana **Nombre del nuevo grupo de administración** que se abre, introduzca el nombre del grupo y haga clic en el botón **Añadir**.

En la jerarquía de grupos de administración, aparecerá un nuevo grupo con el nombre especificado.

*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.

## Reglas de movimiento de dispositivos

Recomendamos que automatice la asignación de dispositivos a grupos de administración mediante *reglas de movimiento de dispositivos*. Una regla de movimiento de dispositivo 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 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, el administrador de Kaspersky Security Center Linux puede crear reglas de movimiento de dispositivos explícitamente en la sección **Activos (dispositivos)** → **Reglas de movimiento**.

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 del grupo dispositivos no asignados solo una vez. Si esta regla movió un dispositivo una vez, la regla nunca lo moverá nuevamente, aun si devuelve el dispositivo al grupo 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 **Mover solo dispositivos que no pertenezcan a ningún 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 de verificación **Mover solo dispositivos que no pertenezcan a ningún grupo de administración** está bloqueada en las propiedades de movimiento que se crean de forma automática. Dichas reglas se crean cuando añade la tarea *Instalar 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 de funcionamiento de Kaspersky Security Center Linux (en particular, en el área de derechos de acceso, eventos e informes). Otra solución se debe encontrar, por ejemplo, a través del uso de perfiles de directiva, tareas para [selecciones de dispositivos](#), asignación de [Agentes de red según el escenario estándar](#), etcétera.

## 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 **Añadir**.
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 dispositivos que no pertenezcan a ningún 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 en cada dispositivo**

La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados.

- **Ejecutar una vez en cada dispositivo y luego cada vez que vuelva a instalar 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 regla permanentemente**

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 reglas**, [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 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 **Detección y despliegue** → **Despliegue y asignación** → **Reglas de movimiento**.

Se muestra la lista de reglas de movimiento.

2. Active la casilla de verificación 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 dispositivos que no pertenezcan a ningún 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 en cada dispositivo**

La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados.

- **Ejecutar una vez en cada dispositivo y luego cada vez que vuelva a instalar 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 regla permanentemente**

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 reglas**, [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 reglas 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 reglas** 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.

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 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 manera 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 manera 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 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 de la distinción entre mayúsculas y minúsculas está configurada para la base de datos que usa para Kaspersky Security Center Linux, mantenga las mayúsculas y minúsculas cuando especifique un nombre de DNS de 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.

- [Rango 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 manera predeterminada.

- [Dirección IP para conectar 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 manera predeterminada.

- [Perfil de conexión modificado](#) 

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 ha cambiado.
- **No se ha seleccionado ningún valor.** La condición no se aplica.

- [Administrado por otro Servidor de administración](#) 

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.
- **No se ha seleccionado ningún valor.** 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 está 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.
- **No se ha seleccionado ningún valor.** 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** o **Servidor de administración de Kaspersky Security Center 15**.

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.

- [Tamaño de bits del sistema operativo](#) ⓘ

Puede seleccionar dispositivos cliente según el tamaño de bits del sistema operativo. En el bloque **Tamaño de bits 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 sondeo** (  ) a la derecha.
3. Seleccione la opción **Tamaño de bits 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 del sistema operativo (en formato *X.Y*), que determinará cómo se aplicará la regla de movimiento al 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.
- **No instalado**. La regla de movimiento de dispositivos solo se aplica a dispositivos móviles sin un certificado para dispositivos móviles.
- **No se ha seleccionado ningún valor**. 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):

- **[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 activada, se aplica una regla de movimiento de dispositivos a los dispositivos de la unidad organizativa del controlador de dominio especificados en la lista que hay debajo de la opción.

Esta opción está deshabilitada de manera predeterminada.

- **[Incluir unidades organizativas secundarias](#)**

Si activa 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 manera predeterminada.

- **Mover dispositivos de las unidades secundarias a los subgrupos correspondientes**
- **Crear subgrupos correspondientes a contenedores de dispositivos detectados recientemente**
- **Eliminar los subgrupos que no se encuentren en el dominio**
- **El dispositivo está incluido en el siguiente grupo de seguridad de dominio **

Si esta opción está activada, se aplica una regla de movimiento de dispositivos a los dispositivos del grupo de seguridad de dominio especificado en la lista que hay debajo de la opción.

Esta opción está deshabilitada de manera predeterminada.

## 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 **Añadir 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 **Añadir 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.



- Especifique el nombre DNS del dispositivo.

El campo del nombre del dispositivo no debe contener caracteres de espacio, caracteres de retroceso, ni los siguientes caracteres prohibidos: , \ / \* ' " ; : & ` ~ ! @ # \$ ^ ( ) = + [ ] { } | < > %

- Haga clic en el botón **Importar dispositivos desde un 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 caracteres de espacio, caracteres de retroceso, 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 procesa la lista de dispositivos y muestra 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.

## Traslado manual de dispositivos o clústeres al grupo de administración

Puede mover dispositivos de un grupo de administración a otro, o del grupo de dispositivos no asignados a un grupo de administración.

También puede trasladar [clústeres o matrices de servidores](#) de un grupo de administración a otro. Cuando traslada un clúster o una matriz de servidores a otro grupo, todos sus nodos se trasladan 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 que se abra en el lado izquierdo.
  - Para abrir el grupo **Dispositivos no asignados**, en el menú principal vaya a **Detección 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 **Matrices de servidores y clústeres**. Abra la pestaña del objeto que desea trasladar.
3. Seleccione las casillas junto a los dispositivos o clústeres que desea mover a un grupo diferente.
4. Haga clic en el botón **Mover a un grupo**.

5. En la jerarquía de grupos de administración, seleccione la casilla junto al grupo de administración al que desea mover los dispositivos o clústeres seleccionados.

6. Haga clic en el botón **Mover**.

Los dispositivos o clústeres seleccionados se mueven al grupo de administración seleccionado.

## Acerca de los clústeres y las matrices de servidores

Kaspersky Security Center Linux admite la tecnología de clústeres. 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 matrices de servidores, la página **Dispositivos administrados** muestra dos pestañas: una para dispositivos individuales y otra para clústeres y matrices 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 **Matrices de servidores y clústeres**.

Los nodos de los clústeres o conjuntos de servidores se enumeran en la pestaña **Dispositivos**, junto con otros dispositivos administrados. Puede [ver propiedades](#) de los nodos como dispositivos individuales y realizar otras operaciones, pero no puede eliminar un nodo de clúster ni trasladarlo a otro grupo de administración por separado de su clúster. Solo puede eliminar o trasladar un clúster completo.

Puede realizar las siguientes operaciones con clústeres o matrices de servidores:

- [Ver propiedades](#)
- [Trasladar el clúster o la matriz de servidores a otro grupo de administración](#)

Cuando traslada un clúster o una matriz de servidores a otro grupo, todos sus nodos se trasladan con él, porque un clúster y cualquiera de sus nodos siempre pertenecen al mismo grupo de administración.

- Eliminar

Es razonable eliminar un clúster o una matriz de servidores solo cuando el clúster o la matriz 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 Linux devuelve el clúster eliminado y sus nodos a la lista de dispositivos administrados automáticamente.

## Propiedades de un clúster o matriz de servidores

*Para ver la configuración de un clúster o una matriz de servidores:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados** → **Matrices de servidores y clústeres**.


Se muestra la lista de clústeres y matrices de servidores.

2. Haga clic en el nombre del clúster o arreglo de servidores requerido.

Se mostrará la ventana de propiedades del clúster o la matriz de servidores seleccionada.

### General

La sección **General** muestra información general sobre el clúster o la matriz de servidores. La información proporcionada se basa en los datos recibidos durante la última sincronización de los nodos de clúster con el Servidor de administración:

- **Nombre**
- **Descripción**
- **[Dominio de Windows](#)** 

Dominio o grupo de trabajo de Windows, que contiene el clúster o la matriz de servidores.

- **[Nombre NetBIOS](#)** 

Nombre de red de Windows del clúster o matriz de servidores.

- **[Nombre DNS](#)** 

Nombre del dominio DNS del clúster o matriz de servidores.

## Tareas

En la pestaña **Tareas**, puede administrar las tareas que se asignan al clúster o matriz de servidores: ver la lista de tareas existentes, crear nuevas, eliminar, iniciar y detener tareas, modificar la configuración de las tareas y ver resultados de ejecución. Las tareas enumeradas se relacionan con la aplicación de seguridad de Kaspersky instalada en los nodos del clúster. Kaspersky Security Center Linux recibe la lista de tareas y los detalles del estado de las tareas de los nodos del clúster. No se mostrará el estado si no se ha establecido una conexión.

## Nodos

Esta pestaña muestra una lista de nodos incluidos en el clúster o matriz 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.

## Ajuste de puntos de distribución y puertas de enlace de conexión

Una estructura de grupos de administración en Kaspersky Security Center Linux 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*.
- 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.

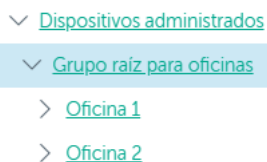
Los siguientes métodos pueden emplearse para armar la estructura de grupos de administración:

- 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 un ordenador 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: Un ordenador portátil incluido en el grupo de administración **Oficina 1** se traslada físicamente a la oficina que corresponde al grupo de administración **Oficina 2**. Después del traslado, el Agente de red del ordenador 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, el ordenador 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.

## 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.

## Asignar puntos de distribución automáticamente

Recomendamos que asigne puntos de distribución automáticamente. En este caso, Kaspersky Security Center Linux seleccionará por sí mismo a qué dispositivos se les deben asignar 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 Linux le permite asignar manualmente dispositivos para actuar como puntos de distribución.

Recomendamos que asigne puntos de distribución automáticamente. En este caso, Kaspersky Security Center Linux seleccionará por sí mismo a qué dispositivos se les deben asignar 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 los parámetros que regulan la interacción del punto de distribución con 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.

- **[Usar 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 IP de difusión múltiple](#)**

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 Linux asigna automáticamente una dirección IP de multidifusión única dentro del rango dado.

- **[Número de puerto de 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 habilitada de manera 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 habilitada de manera predeterminada.

- [Ejecutar servidor push](#) 

En Kaspersky Security Center Linux, un punto de distribución puede funcionar como servidor push para los dispositivos administrados a través del protocolo móvil y los dispositivos gestionados por 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 habilita 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 desocupado.

- En la sección **Alcance**, especifique los grupos de administración a los que el punto de distribución distribuirá las actualizaciones.
- 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 **Descargar del Servidor de administración** para que el punto de distribución pueda recibir actualizaciones del Servidor de administración.
- Seleccione **Utilizar la 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 una tarea** para crearla. Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

- [Descargar archivos de comparación](#) 

Esta opción habilita la función de [descarga de archivos diff](#).

Esta opción está habilitada de manera predeterminada.

- En la subsección **Configuración de la conexión a Internet**, puede especificar la configuración de acceso a Internet:

- [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 utilizar 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 manera 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 utilizar el punto de distribución para reenviar solicitudes de KSN desde los dispositivos administrados:

- [Activar el proxy de KSN en el 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.

Esta opción está deshabilitada de manera predeterminada. Esta opción solo se activa si las opciones **Utilizar el Servidor de administración como servidor proxy** y **Acepto usar Kaspersky Security Network** están activadas 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 de KSN al Servidor de administración](#) 

El punto de distribución envía las solicitudes KSN desde los dispositivos administrados al Servidor de administración.

Esta opción está habilitada de manera predeterminada.

- [Acceder a la nube de KSN/KPSN directamente a través de Internet](#) 

El punto de distribución envía las solicitudes KSN desde los dispositivos administrados a KSN Cloud o 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.

- [Ignorar la configuración del servidor proxy al conectarse a KPSN](#) 

Active 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 la nube de KSN/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 el 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 habilitada de manera 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.

- En la sección **Puerta de enlace de conexión**, puede configurar el punto de distribución a fin de que actúe como 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 manera predeterminada.

- [Establecer conexión a la puerta de enlace 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 el 13299.

Esta opción está disponible si habilita la opción **Establecer conexión a la puerta de enlace desde el Servidor de administración (si la puerta de enlace está en DMZ)**.

- [Abrir puerto para dispositivos móviles \(Autenticación SSL solo para el Servidor de administración\)](#)

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 el 13292. 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. 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 el 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.

- Configure el sondeo del controlador de dominio utilizando el punto de distribución.

- [Sondeo del controlador de dominio](#) 

Puede activar la detección de dispositivos por los controladores de dominio.

Si selecciona la opción **Activar el sondeo de controladores de dominio**, puede seleccionar los controladores de dominio para el sondeo y también especificar la programación de sondeo para ellos.

Si utiliza un punto de distribución de Linux, en la sección **Sondear dominios específicos**, haga clic en **Añadir**, 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 todo el bosque de dominio**
- **Sondear dominios específicos**

- Configure el sondeo de rangos de IP en el punto de distribución.

- [Sondeo de rangos IP](#) 

Puede habilitar el descubrimiento de dispositivos en intervalos IPv4 y en redes IPv6.

Si activa la opción **Activar rango de sondeo**, puede añadir rangos analizados y establecer la programación para ellos. Puede añadir rangos de IP a la lista de intervalos analizados.

Si activa la opción **Usar Zeroconf para sondear las redes IPv6**, el punto de distribución automáticamente sondea la red IPv6 mediante el uso de las [redes de configuración cero](#) (también denominadas *Zeroconf*). 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 sondear las 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 debe utilizar el punto de distribución para almacenar 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 enlace 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. Si desea añadir nuevos puntos de distribución para el grupo de administración, haga clic en el botón **Asignar**.

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.

## Habilitación de un servidor push

En Kaspersky Security Center Linux, un punto de distribución puede funcionar como servidor push para los dispositivos administrados a través del protocolo móvil y los dispositivos gestionados por 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 habilita 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 o 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.

## Acerca de los estados de los dispositivos

Kaspersky Security Center Linux 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 Linux tiene en cuenta el indicador de visibilidad del dispositivo en la red (consulte la tabla a continuación). Si Kaspersky Security Center Linux 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*
- *Correcto* o *Correcto/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.                                                                                                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• Interruptor activado.</li> <li>• Interruptor desactivado.</li> </ul> |
| Demasiados virus detectados                                                            | Una tarea de detección de virus (por ejemplo, la tarea de análisis antimalware) ha detectado algunos virus en el dispositivo y el número de virus encontrados supera el valor especificado.                                                                                                                                                                                                | Más de 0.                                                                                                     |
| El nivel de protección en tiempo real es distinto del 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.                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>• Detenida.</li> <li>• En pausa.</li> <li>• En ejecución.</li> </ul>   |
| No se ha realizado ningún análisis antimalware desde hace mucho tiempo                 | El dispositivo es visible en la red y una aplicación de seguridad está instalada en el dispositivo, pero ni la tarea <i>Análisis de malware</i> ni una tarea de análisis local se ha ejecutado durante 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.                                                                                                 |
| No conectado durante 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 <b>Amenazas activas</b> supera el valor especificado.                                                                                                                                                                                                                                                                                     | Más de 0 elementos.                                                                                           |



|                                                 |                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Se requiere reiniciar                           | 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.                                                                                          | <ul style="list-style-type: none"> <li>• Interruptor desactivado.</li> <li>• Interruptor activado.</li> </ul>                                                                                                                                                                                                                                                                                                       |
| La licencia comercial ha caducado               | El dispositivo es visible en la red, pero la licencia ha caducado.                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• Interruptor desactivado.</li> <li>• Interruptor activado.</li> </ul>                                                                                                                                                                                                                                                                                                       |
| la licencia caduca pronto                       | El dispositivo es visible en la red, pero la licencia instalada en el mismo caduca en menos días que el número de días especificado.                                                                                                                                      | Más de 0 días.                                                                                                                                                                                                                                                                                                                                                                                                      |
| 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.                                                                                                                                          | <ul style="list-style-type: none"> <li>• No cumple con la directiva porque el usuario no dio su consentimiento (solo para dispositivos externos).</li> <li>• No cumple con la directiva debido a un error.</li> <li>• Se debe reiniciar el dispositivo al aplicar la directiva.</li> <li>• No se ha especificado una directiva de cifrado.</li> <li>• No compatible.</li> <li>• Al aplicar la directiva.</li> </ul> |
| Problemas de seguridad no procesados detectados | Se han encontrado problemas de seguridad sin procesar en el dispositivo. Los problemas de seguridad pueden ser creados manualmente por el administrador o automáticamente por las aplicaciones de Kaspersky administradas que se han instalado en el dispositivo cliente. | <ul style="list-style-type: none"> <li>• Interruptor desactivado.</li> <li>• Interruptor activado.</li> </ul>                                                                                                                                                                                                                                                                                                       |

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                               |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Estado del dispositivo definido por la aplicación      | El estado del dispositivo es definido por la aplicación administrada.                                                                                                                                                                                                                                                                                                                                                       | <ul style="list-style-type: none"> <li>• Interruptor desactivado.</li> <li>• Interruptor activado.</li> </ul> |
| El dispositivo no tiene espacio disponible 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 <i>Crítico</i> o <i>Advertencia</i> cambiarán por el estado <i>Sin inconvenientes</i> 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.                                                                                                  |
| Se ha perdido la conexión con el dispositivo           | 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.                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>• Interruptor desactivado.</li> <li>• Interruptor activado.</li> </ul> |
| La protección está desactivada                         | El dispositivo es visible en la red, pero la aplicación de seguridad del dispositivo ha estado deshabilitada por un tiempo superior al especificado.<br><br>En este caso, el estado de la aplicación de seguridad es <i>detenida</i> o <i>error</i> , y difiere del siguiente: <i>iniciada</i> , <i>en ejecución</i> o <i>suspendida</i> .                                                                                  | Más de 0 minutos.                                                                                             |
| La aplicación de seguridad no se está ejecutando       | El dispositivo es visible en la red y tiene instalada una aplicación de seguridad, pero esa aplicación no se está ejecutando.                                                                                                                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>• Interruptor desactivado.</li> <li>• Interruptor activado.</li> </ul> |

Kaspersky Security Center Linux le permite configurar el cambio automático 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 especificadas. 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 Linux 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.

Quando Kaspersky Security Center Linux asigna un estado a un dispositivo, para algunas condiciones (consulte la columna Descripción de la condición) se tiene en cuenta el indicador de visibilidad. 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*.

## 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 **Asignar Crítico si se especifican**, 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. Configure el valor necesario para la condición seleccionada.  
Puede establecer valores para algunas condiciones pero no para todas.
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 **Asignar Advertencia si se especifican**, 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. Configure el valor necesario para la condición seleccionada.  
Puede establecer valores para algunas condiciones pero no para todas.
5. Haga clic en **Aceptar**.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Advertencia* al dispositivo administrado.

## 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 Linux proporciona una amplia gama de *selecciones predefinidas* (por ejemplo, **Dispositivos con el estado Crítico, La protección está desactivada, 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 Linux 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 **Detección 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 **Añadir**.

Se abre la ventana **Configuración de 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 **Añadir**.

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 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 la selección](#)

Si habilita esta opción, la condición elegida se aplicará a la inversa. La selección incluirá todos los dispositivos que no cumplan con la condición.

Esta opción está deshabilitada de manera predeterminada.

## 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 grupo de trabajo especificado.

- [Grupo de administración](#) 

Muestra los dispositivos incluidos en el grupo de administración especificado.

- [Descripción](#) 

Texto de la ventana de propiedades del dispositivo: en el campo **Descripción** de la sección **General**.

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 frases como **SUSE Linux Enterprise Server 12** o **SUSE Linux Enterprise Server 15**, puedes ingresar **SUSE Linux Enterprise Server 1?**.

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.

- [Rango 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 manera predeterminada.

- [Administrado por otro Servidor de administración](#) 

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.
- **No se ha seleccionado ningún valor.** La condición no se aplica.

En la subsección **Controlador de dominio**, puede configurar los criterios para incluir dispositivos en una selección según la pertenencia al dominio:

- [El dispositivo se encuentra en una unidad organizativa de dominio](#) 

Si activa esta opción, la selección incluirá los dispositivos de la unidad organizativa de dominio especificada en el campo de entrada.

Esta opción está deshabilitada de manera predeterminada.

- [El dispositivo es miembro del grupo de seguridad de dominio](#) 

Si activa 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 manera 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.
- **No se ha seleccionado ningún valor.** 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:

- **Activado.** La selección incluirá dispositivos en los que esté activada la casilla **No desconectar del Servidor de administración**.
- **Desactivado.** 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.
- **No se ha seleccionado ningún valor.** El criterio no se aplicará.

- [Última conexión al 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.

- [El sondeo de la red ha detectado dispositivos nuevos](#)

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 manera predeterminada.

- [El dispositivo es 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.
- **No se ha seleccionado ningún valor.** El criterio no se aplicará.

## 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: *Aceptar, 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: *Aceptar, Crítico o Advertencia*.

En la sección **Estado de los 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 la prevención contra fugas de datos](#)

Buscar dispositivos basándose en el estado de Prevención de fuga de datos (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

- [Estado de la protección de los servidores de colaboración](#)

Buscar dispositivos basándose en el estado de la protección para servidores de colaboración (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

- [Estado de la protección antivirus de servidores de correo](#)

Buscar dispositivos basándose en el estado de la protección para servidores de correo (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

- [Estado de Sensor de Endpoint](#)

Buscar dispositivos basándose en el estado del componente Sensor de Endpoint (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

En la sección **Problemas relacionados con el estado de 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.

## Detalles 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 del sistema operativo (en formato *X.Y*), que determinará cómo se aplicará la regla de movimiento al dispositivo. De manera predeterminada, no hay una versión definida.

- [Tamaño de bits 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):

- [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](#)** 

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). Los ordenadores 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 reloj de la CPU, en MHz, de](#)**

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.

- **[Frecuencia de reloj de la CPU, en MHz, a](#)**

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 virtual, de](#)**

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 virtual, a](#) <sup>?</sup>

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, de](#) <sup>?</sup>

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 del disco duro, en GB, hasta](#) <sup>?</sup>

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, de](#) <sup>?</sup>

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, a](#) <sup>?</sup>

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 del 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](#) <sup>?</sup>

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](#) <sup>?</sup>

Campo de entrada en el que puede especificar la versión de la aplicación seleccionada.

- [Proveedor](#) <sup>?</sup>

Lista desplegable en la que puede seleccionar el desarrollador de una aplicación instalada en el dispositivo.

- [Estado de la aplicación](#) <sup>?</sup>

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 la 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 manera 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 la 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 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 manera 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:

#### [El WUA se ha cambiado 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** 

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.

- **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.

- **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** 

En la lista desplegable, puede incluir en la selección los dispositivos administrados mediante Kaspersky Security Center Linux:

- **Sí.** En la selección los dispositivos administrados mediante Kaspersky Security Center Linux.
- **No.** La aplicación incluye en la selección dispositivos que no estén administrados por Kaspersky Security Center Linux.
- **No se ha seleccionado ningún valor.** 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.
- **No se ha seleccionado ningún valor.** 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:

- **[Fecha de publicación de las bases de datos](#)** ⓘ

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 manera predeterminada.

- **[Número de 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 manera predeterminada.

- **[Último análisis](#)** ⓘ

Si esta casilla está activada, se puede hacer una búsqueda de dispositivos cliente por la fecha de último análisis antimalware. En los campos de entrada puede especificar el período de tiempo en el cual se realizó el último análisis antimalware.

Esta opción está deshabilitada de manera 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 manera 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 la aplicación** 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 la aplicación**, 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 la versión del componente seleccionado deberá ser igual, anterior o posterior a ese valor. 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 manera predeterminada.

Para agregar etiquetas al criterio, haga clic en el botón **Añadir** 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.

- [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.

- [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).

## 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 Linux le permite guardar información sobre los dispositivos desde una selección de dispositivos y exportarla como archivo CSV o TXT.

*Para exportar la lista de dispositivos de la 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 ha aplicado 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 **Detección 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

En esta sección, se brinda una descripción de las etiquetas para dispositivos y se ofrecen instrucciones para crearlas y modificarlas, así como para etiquetar dispositivos de forma manual o automática.

## Acerca de las etiquetas de dispositivo

Kaspersky Security Center Linux permite que usted *etiquete* dispositivos. Una etiqueta es un identificador de un dispositivo que se puede utilizar para agrupar, describir o encontrar dispositivos. Pueden utilizarse para crear [selecciones](#), hallar dispositivos específicos y distribuir dispositivos en [grupos de administración](#).

Puede etiquetar dispositivos manual o automáticamente. Utilice el etiquetado manual para rotular dispositivos puntuales. Kaspersky Security Center Linux realiza el etiquetado automático de acuerdo con las reglas de etiquetado especificadas.

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 [CentOS] a todos los dispositivos con el sistema operativo CentOS. A continuación, puede usar esta etiqueta al crear una selección de dispositivos. Esto le ayudará a clasificar todos los dispositivos CentOS y a asignarles una tarea.

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 **Añadir**.  
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 una 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.

La lista de dispositivos que aparece muestra solo los dispositivos que tienen asignada la etiqueta.

Para regresar a la lista de etiquetas de dispositivo, haga clic en el botón **Atrás** de su navegador.

## 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.

Puede [asignar otra etiqueta](#) al dispositivo o [quitarle una etiqueta que tenga asignada](#). También puede ver una lista con todas las etiquetas de dispositivo creadas en el Servidor de administración.

## 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 **Añadir**.
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 **Correcto** 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. Active la casilla de verificación adyacente a la etiqueta que desee quitar del dispositivo.
5. Al principio de la lista, haga clic en el botón **Desasignar 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 klsclag.

## Ver las reglas de etiquetado automático de dispositivos

*Para ver las reglas que se utilizan para etiquetar dispositivos automáticamente,*

Realice cualquiera 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 haga clic en el enlace **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 cualquiera de las siguientes acciones:
    - Pase el interruptor a **Regla activada** para habilitar la regla.
    - Pase el interruptor a **Regla desactivada** para deshabilitar la regla.
4. Realice cualquiera de las siguientes acciones:
  - Si desea agregar una condición, haga clic en el botón **Añadir** 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, active 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 **Añadir**.

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 activada** para habilitar la regla.
- Pase el interruptor a **Regla desactivada** 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 **Añadir** 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:** Propiedades de red del dispositivo, como el nombre DNS del dispositivo o la inclusión del dispositivo en una subred IP.

Si la intercalación de la distinción entre mayúsculas y minúsculas está configurada para la base de datos que usa para Kaspersky Security Center Linux, mantenga las mayúsculas y minúsculas cuando especifique un nombre de DNS de 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.
- **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](#).
- Después de que el Servidor de administración detecte un cambio en la configuración de un dispositivo que cumpla las condiciones de la regla o 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. Active la casilla de verificación 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](#).

## Protección y cifrado de datos

El cifrado de datos reduce el riesgo de fugas no intencionadas de datos confidenciales y corporativos en caso de robo o pérdida de su equipo portátil o disco duro. Además, el cifrado de datos le permite evitar el acceso de usuarios y aplicaciones no autorizados.

Puede usar la función de cifrado de datos si su red incluye dispositivos administrados basados en Windows con Kaspersky Endpoint Security para Windows instalado. En este caso, puede gestionar 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, usted puede, por ejemplo, [activar o desactivar el cifrado](#), [ver la lista de unidades cifradas](#) o [generar y ver informes sobre el cifrado](#).

Para configurar el cifrado, defina la directiva de Kaspersky Endpoint Security para Windows en Kaspersky Security Center Linux. 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](#).

Actualmente, la administración de cifrado para una jerarquía de Servidores de administración no está disponible en Web Console. Utilice el Servidor de administración principal para administrar dispositivos cifrados.

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.

## Ver la lista de unidades cifradas

En Kaspersky Security Center Linux puede ver detalles sobre unidades cifradas y sobre dispositivos cifrados en el nivel de unidad. 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** → **Dispositivos cifrados**.

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 Linux 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 visualizar informes sobre cifrado

Puede generar los siguientes informes:

- Informe sobre el estado del 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, por ejemplo, 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 del 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 los derechos de acceso a dispositivos cifrados. Este informe muestra qué cuentas de usuario tienen acceso a unidades cifradas.
- Informe sobre errores en el cifrado de archivos. Este informe contiene información sobre errores que han ocurrido durante tareas de cifrado o descifrado de datos en dispositivos.
- Informe sobre el bloqueo del acceso a 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 **Control e informes** → **Informes**. Alternativamente, en la sección **Operaciones** → **Protección y cifrado de datos**, puede generar los siguientes informes de cifrado:

- Informe sobre el estado del cifrado de los dispositivos de almacenamiento masivo
- Informe sobre los derechos de acceso a dispositivos cifrados
- Informe sobre errores en el 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 el menú principal, vaya a **Operaciones** → **Protección y cifrado de datos**.
3. Seleccione una de las siguientes secciones:
  - **Dispositivos cifrados** genera el Informe sobre el estado del cifrado de los dispositivos de almacenamiento masivo o el informe sobre los derechos de acceso a dispositivos cifrados.
  - **Eventos de cifrado** genera el Informe sobre errores en el cifrado de archivos.
4. 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** → **Dispositivos cifrados**. Aparece una lista de unidades cifradas.
3. Seleccione la unidad a la que el usuario haya solicitado acceso.
4. Haga clic en el botón **Conceder acceso al dispositivo en modo desconectado**:
5. En la ventana que se abre, seleccione el complemento Kaspersky Endpoint Security para Windows.
6. Siga las instrucciones proporcionadas en la [Ayuda de Kaspersky Endpoint Security para Windows](#) (consulte las instrucciones para Kaspersky Security Center Web Console 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.

## Cambiar los dispositivos cliente de Servidor de administración

Para dispositivos cliente específicos, puede cambiar el Servidor de administración a otro. Para ello, utilice la tarea *Cambiar Servidor de administración*.

*Para cambiar el Servidor de administración que administra ciertos dispositivos cliente:*

1. Conéctese al Servidor de administración que administra los dispositivos.
2. [Cree](#) la tarea de cambio del Servidor de administración.

Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente. En la ventana **Nueva tarea** del asistente para crear nueva tarea, seleccione la aplicación **Kaspersky Security Center 15** y el tipo de tarea **Cambiar Servidor de administración**. Después, especifique los dispositivos para los que desea cambiar el Servidor de administración:

- [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.

- [Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista](#)

Puede especificar nombres DNS, direcciones IP y subredes IP de dispositivos a los cuales debe asignar la tarea.

Puede 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 en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred 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 resultarle útil para, por ejemplo, ejecutar una tarea en dispositivos que tengan una versión específica de un sistema operativo.

### 3. 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.

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 obtener descripciones detalladas sobre los escenarios en los que no se proporciona ningún acceso a datos cifrados, consulte la [Ayuda de Kaspersky Endpoint Security para Windows](#).

## 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 habilitada de manera predeterminada.

- [Forzar la herencia de la 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 manera predeterminada.

5. En la sección **Actividad de los dispositivos**, active o deshabilite las siguientes opciones:

- [\*\*Notificar al administrador si el dispositivo ha estado inactivo durante 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 habilitada de manera predeterminada.

- [\*\*Quitar el dispositivo del grupo si ha estado inactivo durante 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 habilitada de manera predeterminada.

6. Haga clic en **Guardar**.

Se guardarán y aplicarán los cambios.

## Envío de mensajes a usuarios de dispositivos

*Para enviar un mensaje por correo electrónico a usuarios de dispositivos:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Añadir**.  
Se inicia el Asistente para crear nueva tarea.
3. En la lista desplegable **Tipo de tarea**, seleccione **Enviar mensaje al usuario**.
4. Seleccione una opción para elegir el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplicará la tarea.
5. Ejecute la tarea creada.

Una vez finalizada la tarea, el mensaje creado se enviará a los usuarios de los dispositivos seleccionados. La tarea **Enviar mensaje al usuario** solo está disponible para dispositivos que funcionan con Windows.

## Encendido, apagado y reinicio remoto de dispositivos cliente

Kaspersky Security Center Linux le permite administrar dispositivos cliente de manera remota al activarlos, apagarlos o reiniciarlos.



*Para administrar remotamente dispositivos cliente:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Añadir**.  
Se inicia el Asistente para crear nueva tarea.
3. En la lista desplegable **Tipo de tarea**, seleccione **Administrar dispositivos**.
4. Seleccione una opción para elegir el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplicará la tarea.
5. Seleccione el comando (encender, apagar o reiniciar). Opcionalmente, especifique el mensaje de solicitud del usuario y la opción **Tiempo de espera antes del cierre forzado de aplicaciones en sesiones bloqueadas (min)** para los comandos de apagado y reinicio.
6. Ejecute la tarea creada.

Luego de finalizar la tarea, se ejecutará el comando (encender, apagar o reiniciar) en los dispositivos seleccionados.

# Despliegue de las aplicaciones de Kaspersky

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

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 necesarios manualmente.

Las siguientes aplicaciones pueden desplegarse a través de Kaspersky Security Center Web Console:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security para Windows

## Etapas

El despliegue de las aplicaciones de Kaspersky se divide en etapas:

### 1 Descargar el complemento de administración web para la aplicación

Esta etapa forma parte del asistente de inicio rápido. Si elige no ejecutar el asistente, descargue los complementos manualmente.

### 2 Descarga y creación de paquetes de instalación

Esta etapa forma parte del asistente de inicio rápido.

El asistente de inicio rápido le permite descargar el paquete de instalación con el complemento web de administración. Si no seleccionó esta opción al ejecutar el asistente o si no lo ejecutó, debe [descargar el paquete manualmente](#).

Si no puede instalar las aplicaciones de Kaspersky mediante Kaspersky Security Center Linux en algunos dispositivos, (por ejemplo, en dispositivos de empleados remotos) 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.

Como alternativa, puede [descargar los paquetes de distribución para el Agente de red y las aplicaciones de seguridad del sitio web de Kaspersky](#)<sup>[2]</sup>. Si, por algún motivo, no es posible realizar la instalación remota de las aplicaciones, puede usar los paquetes de distribución descargados para instalar las aplicaciones localmente.

### 3 Creación, configuración y ejecución de la tarea de instalación remota

Este paso forma parte del asistente de despliegue de la protección. Si decide no ejecutar el asistente de despliegue de la protección, [debe crear esta tarea manualmente](#) y configurarla también 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.

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.

#### 4 Creación y configuración de tareas

La tarea de *actualización* de Kaspersky Endpoint Security debe estar configurada.

Este paso forma parte del asistente de inicio rápido: la tarea se crea y configura automáticamente con la configuración predeterminada. Si no ejecutó el asistente, [debe crear esta tarea manualmente](#) y configurarla del mismo modo. Si utiliza el Asistente de inicio rápido, asegúrese de que la [programación de la tarea](#) cumpla con sus requisitos. (De forma predeterminada, el inicio programado para la tarea se establece en **Manualmente**, pero es posible que desee elegir otra opción).

#### 5 Creando directivas

Cree la directiva para Kaspersky Endpoint Security for Linux [de forma manual](#) o 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.

#### 6 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.

## Añadir complementos para aplicaciones de Kaspersky

Para desplegar una aplicación Kaspersky, como Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security para Windows, debe añadir e instalar el complemento de administración de la aplicación.

*Para descargar un complemento web de administración para una aplicación de Kaspersky:*

1. En el menú principal, vaya a **Configuración** → **Complementos web**.
2. En la ventana que se abre, haga clic en el botón **Añadir**.  
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 for Linux) haciendo clic en su nombre.  
Se muestra una página de descripción del complemento.
4. En la página de descripción del complemento, haga clic en **Instalar 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 web de administración desde el [sitio web de Kaspersky](#).

*Para descargar o actualizar complementos web de administración desde un archivo, siga estos pasos:*

1. En el menú principal, vaya a **Configuración** → **Complementos web**.
2. Especifique el archivo del complemento y la firma del archivo:
  - Haga clic en **Añadir 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 web de administración se descarga del archivo y se muestra en la lista de complementos web 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 **Detección 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 **Añadir**.

Se inicia el Asistente de nuevo paquete. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. En la primera página del asistente, seleccione la opción **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 Linux.

- Haga clic en el nombre de un paquete de instalación; por ejemplo, Kaspersky Endpoint Security for Linux. 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.

- 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 el 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 continuar con el siguiente paso de la instrucción. Si cierra la ventana del asistente, el proceso de descarga continuará en segundo plano.

Si desea controlar la descarga del paquete de instalación:

- En el menú principal, vaya a **Operaciones** → **Repositorios** → **Paquetes de instalación** → **En curso ()**.
- Consulte las columnas **Progreso de la descarga** y **Estado de la 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 **Descargados**. 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](#).

- Para algunas aplicaciones de Kaspersky, durante el proceso de descarga, se muestra el botón **Mostrar el EULA**. Si ve este botón, haga lo siguiente:

- Haga clic en el botón **Mostrar el EULA** para leer el Contrato de licencia de usuario final (EULA).
- 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.

- 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.

## Crear paquetes de instalación a partir de un archivo

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. Realice una de las siguientes acciones:

- En el menú principal, vaya a **Detección 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 **Añadir**.

Se inicia el Asistente de nuevo paquete. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En la primera página del asistente, seleccione **Crear un paquete de instalación a partir de un archivo**.

4. En la siguiente página del asistente, especifique el nombre del paquete y haga clic en el botón **Examinar**.

5. En la ventana que se abre, 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.

Se inicia la carga de archivos en el Servidor de administración.

6. Si especificó un archivo de una aplicación de Kaspersky, es posible que se le pida que lea y acepte el [Contrato de licencia de usuario final](#) (EULA) de la aplicación. Para continuar, debe aceptar el EULA. Seleccione la opción **Aceptar los términos y las condiciones de este Contrato de licencia de usuario final** solo si ha leído, comprende y acepta en su totalidad los términos del EULA.

Además, es posible que se le solicite que lea y acepte la [Política de privacidad](#). Para continuar, debe aceptar la Política de privacidad. Seleccione la opción **Acepto la Política de privacidad** solo si entiende y está de acuerdo con que sus datos serán manejados y transmitidos (incluso a terceros países) como se describe en la Política de privacidad.

7. En la página siguiente del asistente, seleccione un archivo (de la lista de archivos extraídos del archivo de almacenamiento seleccionado) 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 informa de la finalización del proceso.

Si no se crea el paquete de instalación, se muestra el mensaje adecuado.

8. 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 de un 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 los parámetros de la línea de comandos.

## 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 usted puede almacenar en el servidor web, en una carpeta compartida, enviar por correo electrónico o transferir al dispositivo cliente de otra manera. En el dispositivo cliente, el usuario puede ejecutar el archivo recibido localmente para instalar una aplicación sin utilizar Kaspersky Security Center Linux. Puede crear paquetes de instalación independientes de aplicaciones de Kaspersky y de aplicaciones de terceros. 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 terceras personas.

*Para crear un paquete de instalación independiente:*

1. Realice una de las siguientes acciones:
  - En el menú principal, vaya a **Detección 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 **Mediante un paquete independiente**.

Se inicia el Asistente para crear paquete de instalación independiente. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

4. En la primera página del asistente, asegúrese de seleccionar la opción **Instalar Agente de red junto con esta aplicación** si desea instalar el Agente de red junto con la aplicación seleccionada.

Esta opción está habilitada de manera predeterminada. Le 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.

Si la aplicación seleccionada ya cuenta con un paquete de instalación independiente en el Servidor de administración, el asistente se lo informa. Si esto sucede, elija una de estas acciones:

- **Crear un paquete de instalación independiente.** Seleccione esta opción, por ejemplo, si 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 paquete de instalación independiente existente.** Seleccione esta opción si desea utilizar un paquete de instalación independiente que ya exista. El proceso para crear paquetes no se iniciará.
- **Crear de nuevo un paquete de instalación independiente existente.** 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 página del asistente **Mover a lista de dispositivos administrados**, la opción **No mover dispositivos** está seleccionada de forma predeterminada. Si no desea mover el dispositivo cliente a ningún grupo de administración después de la instalación del Agente de red, no cambie la selección de la opción.

Si desea mover los dispositivos cliente después de la instalación del Agente de red, seleccione la opción **Mover 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. En la página siguiente del asistente, cuando haya finalizado el proceso de creación del paquete de instalación independiente, 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.

## 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, ejecute el símbolo del sistema con la cuenta que se usó para [instalar el Servidor de administración](#).
2. Cambie su directorio actual a la carpeta de instalación de Kaspersky Security Center Linux (normalmente, /opt/kaspersky/ksc64/sbin).
3. Según el tipo de instalación del Servidor de administración, introduzca uno de los siguientes comandos en la cuenta raíz:

- 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 Linux:

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <número de bytes > --stp
klfoc
```

Donde <número de bytes> es un número de bytes en formato hexadecimal o decimal.

Por ejemplo, si el límite requerido es de 2 GB, puede especificar el valor decimal 2147483648 o el valor hexadecimal 0x80000000. En este caso, para una instalación local del Servidor de administración, puede usar 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.

## 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.
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. Asigne el nombre completo del archivo de respuestas (con su ruta de acceso) a la variable de entorno KLAUTOANSWERS. Use para ello un comando como el siguiente:

```
export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
```

5. Cree el archivo de respuestas (en formato TXT) en el directorio al que apunte la variable de entorno. 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](#) 

| 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: Confirmando 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                                                                                                                      |

|                     |    |                                                                                                                        |                                                                                                                                                                                                                                                                                                                  |
|---------------------|----|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     |    |                                                                                                                        | <p>existente (no se usará una puerta de enlace de conexión en la primera llamada).</p> <p>2: No usar una puerta de enlace de conexión.</p> <p>3: Usar una puerta de enlace de conexión.</p> <p>4: La instancia de Agente de red actuará como puerta de enlace de conexión en una zona desmilitarizada (DMZ).</p> |
| 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.                                                                                                                                                                                                                                                                                       |

#### 6. Instale el Agente de red:

- Para instalar el Agente de red con un paquete RPM en un sistema operativo de 32 bits, ejecute el siguiente comando:  

```
rpm -i klnagent-<número de compilación>.i386.rpm
```
- Para instalar el Agente de red con un paquete RPM en un sistema operativo de 64 bits, ejecute el siguiente comando:  

```
rpm -i klnagent64-<número de compilación>.x86_64.rpm
```
- Para instalar el Agente de red con un paquete RPM en un sistema operativo de 64 bits para la arquitectura ARM, ejecute el siguiente comando:  

```
rpm -i klnagent64-<número de compilación>.aarch64.rpm
```
- Para instalar el Agente de red con un paquete DEB en un sistema operativo de 32 bits, ejecute el siguiente comando:  

```
apt-get install ./klnagent_<número de compilación>.i386.deb
```
- Para instalar el Agente de red con un paquete DEB en un sistema operativo de 64 bits, ejecute el siguiente comando:  

```
apt-get install ./klnagent_<número de compilación>.amd64.deb
```
- Para instalar el Agente de red con un paquete DEB en un sistema operativo de 64 bits para la arquitectura ARM, ejecute el siguiente comando:  

```
apt-get install ./klnagent64_<número de compilación>.arm64.deb
```

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](#).

Antes de comenzar:

- Asegúrese de que el dispositivo en el que desea instalar Network Agent for Linux cuente con una de las [distribuciones de Linux compatibles](#).
- Descargue el archivo de instalación del Agente de red necesario del [sitio web de Kaspersky](#).

Ejecute los comandos provistos en esta instrucción bajo una cuenta con privilegios de raíz.

*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 especifique el siguiente ajuste:

```
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 `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` 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 Linux no incluye la clave de la aplicación `kaspersky_astra_pub_key.gpg`, puede descargarla haciendo clic en el enlace:

[https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky\\_astra\\_pub\\_key.gpg](https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg).

5. Actualice los discos RAM:

```
update-initramfs -u -k all
```

Reinicie el sistema.

6. Lleva a cabo los [pasos de preparación comunes para cualquier dispositivo Linux](#).

El dispositivo está preparado. Ahora puede proceder a la [instalación del Agente de red](#).

## 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.
- **Archivo hash.** 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 **Anular 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**.

## Distribución de paquetes de instalación a servidores de administración secundarios

Kaspersky Security Center Linux le permite [crear paquetes de instalación](#) para aplicaciones de Kaspersky y de terceros, así como distribuir paquetes de instalación a dispositivos cliente e instalar aplicaciones desde los 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 **Añadir**.  
Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
4. En la página **Nueva tarea**, en la lista desplegable **Aplicación**, 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 **Cobertura 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 tareas**, 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.

## 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 siguiente software esté instalado en el dispositivo Linux de destino:

- Sudo
- Intérprete del lenguaje Perl versión 5.10 o posterior

2. 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 la configuración siguiente tenga los valores 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 con 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. Use el comando `visudo` en sudo para abrir el archivo de configuración de sudoers.

En el archivo abierto, encuentre la línea que comienza con `%sudo` (o con `%wheel` si utiliza el sistema operativo CentOS). En esta línea, especifique lo siguiente: `<nombre_de_usuario> ALL = (ALL) NOPASSWD: ALL`. En este caso, `<nombre_de_usuario>` es la cuenta de usuario que se utilizará para conectar el dispositivo mediante SSH. Si está utilizando el sistema operativo Astra Linux, en el archivo `/etc/sudoers` añada una última línea con el siguiente texto: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

d. Guarde el archivo `sudoers` y, luego, ciérrelo.

- e. Conéctese al dispositivo de nuevo a través de SSH y asegúrese de que el servicio de Sudo no le solicite introducir una contraseña, porque puede usar el comando `sudo whoami` para hacerlo.

3. Abra el archivo `/etc/systemd/logind.conf` file, y ejecute una de las siguientes acciones:

- Especifique "no" como valor para la configuración KillUserProcesses: `KillUserProcesses=no`.
- Para el ajuste KillExcludeUsers, escriba el nombre de usuario de la cuenta con la que se va a realizar la instalación remota, por ejemplo, `KillExcludeUsers=root`.

Si el dispositivo de destino ejecuta Astra Linux, añada la cadena `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` en el archivo `/home/< nombre_de_usuario >/.bashrc`, en el que `< nombre_de_usuario >` es la cuenta de usuario que se utilizará para conectar el dispositivo mediante SSH.

Para aplicar el ajuste modificado, reinicie el dispositivo Linux o ejecute el siguiente comando:

```
$ sudo systemctl restart systemd-logind.service
```

4. 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.
5. 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](#).

## 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. Descargue el paquete de instalación del Agente de red [mediante la interfaz de la aplicación](#) o desde el [sitio web de Kaspersky](#).
- c. Para crear un paquete de instalación remota, use los archivos siguientes:
  - `klagent.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, marque la casilla **Usando los recursos del sistema operativo mediante el Servidor de administración**. Quite la selección a todo.
- En la página **Seleccionar 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 medio ambiente: `-m, -p, --preserve-environment`.

Se puede arrojar un error si instala Agente de red con SSH en dispositivos que ejecutan versiones de Fedora anteriores a la versión 20. En este caso, para que Agente de red se instale correctamente, comente la opción `Defaults requiretty` (enciérrela en la sintaxis de comentarios para eliminarla del código que se ejecutará) en el archivo `/etc/sudoers`. Para una descripción detallada de la condición de la opción `Defaults requiretty`, que puede causar problemas durante la conexión mediante SSH, consulte el [sitio web de Bugzilla \(sistema de seguimiento de errores\)](#).<sup>[2]</sup>

## Instalar aplicaciones mediante la tarea de instalación remota

Kaspersky Security Center Linux permite instalar aplicaciones en dispositivos remotamente con tareas de instalación remota. Esas tareas se crean y se asignan a dispositivos a través de un asistente dedicado. Para asignar una tarea a dispositivos de modo más fácil y rápido, puede especificar dispositivos en la ventana del asistente de una de estas formas:

- **Seleccionar dispositivos de 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 direcciones de dispositivo manualmente o importar direcciones desde una lista.** Puede especificar nombres DNS, direcciones IP y subredes IP de 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 ya 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 una instalación remota correcta en el dispositivo en el cual no se ha instalado ningún Agente de red, se deben abrir los siguientes puertos: a) TCP 139 y 445; b) UDP 137 y 138. De manera predeterminada, estos puertos se abren en todos los dispositivos incluidos en el dominio. La [utilidad de preparación para instalaciones remotas](#) los abre automáticamente.

## Instalación de una aplicación de forma remota

Esta sección contiene información sobre cómo instalar de forma remota una aplicación en dispositivos de un grupo de administración, en dispositivos con direcciones específicas o en una selección de dispositivos.

*Para instalar una aplicación en dispositivos específicos:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Añadir**.  
Se inicia el Asistente para crear nueva tarea.
3. En la sección **Tipo de tarea**, seleccione **Instalar aplicación en remoto**.
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.

- [Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista](#) 

Puede especificar nombres DNS, direcciones IP y subredes IP de dispositivos a los cuales debe asignar la tarea.

Puede 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 en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred 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 resultarle útil para, por ejemplo, ejecutar una tarea en dispositivos que tengan una versión específica de un sistema operativo.

La tarea *Instalar aplicación en remoto* se crea para los dispositivos especificados. Si seleccionó la opción **Asignar tarea a un grupo de administración**, la tarea es grupal.

5. En el paso **Cobertura de la tarea**, especifique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

Los ajustes disponibles dependen de la opción seleccionada en el paso anterior.

6. En el paso **Paquetes de instalación**, especifique la siguiente configuración:

- En el campo **Seleccione un paquete de instalación**, seleccione el paquete de instalación de una aplicación que desea 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:

- [Usando 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.

- [Usando los recursos del sistema operativo mediante 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.

Esta opción se habilita de manera predeterminada para las tareas de instalación remota creadas en servidores de administración virtuales.

La única forma de instalar una aplicación para Windows (incluido el Agente de red para Windows) en un dispositivo que no tenga instalado el Agente de red es mediante un punto de distribución basado en Windows. Por lo tanto, cuando instale una aplicación de Windows:

- Seleccione esta opción.
- Asegúrese de que se asigne un punto de distribución para los dispositivos cliente de destino.
- Asegúrese de que el punto de distribución esté basado en Windows.

- [Usando los recursos del sistema operativo mediante el 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 habilitada de manera predeterminada.

- En el campo **Número máximo de descargas concurrentes**, especifique el número máximo permitido de dispositivos cliente a los que el Servidor de administración puede transmitir simultáneamente los archivos.
- En el campo **Número máximo de intentos de instalación**, especifique el número máximo permitido de ejecuciones del instalador.

Si se excede la cantidad de intentos especificados en el parámetro, Kaspersky Security Center Linux deja de iniciar el instalador en el dispositivo. Para reiniciar la tarea *Instalar la aplicación de forma remota*, aumente el valor del parámetro **Número máximo de intentos de instalación** e inicie la tarea. O bien, puede crear una nueva tarea *Instalar aplicación de forma remota*.

- Defina la configuración adicional:

- [No reinstalar la aplicación si ya se encuentra 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 habilitada de manera predeterminada.

- [Verificar el tipo de sistema operativo antes de descargar](#) 

Antes de transmitir los archivos a los dispositivos cliente, Kaspersky Security Center Linux verifica si la configuración de la utilidad de Instalación puede aplicarse al sistema operativo del dispositivo cliente. Si la configuración no puede aplicarse, Kaspersky Security Center Linux 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.

- **Indicar 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 manera predeterminada.

- Seleccione en qué dispositivos desea 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.

- Especifique si los dispositivos deben moverse a un grupo de administración después de la instalación.

- **No mover 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 al grupo seleccionado (solo se puede seleccionar un único grupo)** ⓘ

Los dispositivos se moverán al grupo de administración que seleccione.

Tenga en cuenta que la opción **No mover dispositivos** está seleccionada de forma predeterminada. Es posible que quiera mover los dispositivos manualmente por seguridad.

7. En este paso del asistente, especifique si los dispositivos deben reiniciarse durante la instalación de las 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.

8. Si es necesario, en el paso **Seleccionar cuentas para acceder a los dispositivos**, añada las cuentas que se utilizarán para iniciar la tarea *Instalar aplicación en remoto*:

- [No es necesaria una cuenta \(Agente de red instalado\)](#) 

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 ha instalado en los dispositivos cliente.

- [Se necesita una cuenta \(no se utiliza Agente de red\)](#) 

Seleccione esta opción si el Agente de red no está instalado en los dispositivos a los que asigna la tarea de instalación remota. En ese caso, puede indicar una cuenta de usuario para instalar la aplicación.

Para especificar la cuenta de usuario con la que se ejecutará el instalador de la aplicación, haga clic en el botón **Añadir**, 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.

9. En el paso **Finalizar la creación de tareas**, 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. En esta ventana puede comprobar los parámetros de las tareas, modificarlos o programar inicios de tareas si es necesario.

10. En la lista de tareas, seleccione la tarea que ha creado y haga clic en **Iniciar**.

También puede esperar a que la tarea se inicie de acuerdo con la programación que ha especificado en la configuración de la tarea.

Cuando se completa la tarea de instalación remota, la aplicación seleccionada se instala en los dispositivos especificados.

## 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 la aplicación en Servidor de administración secundario de forma remota**.  
El Asistente para crear nueva tarea crea una tarea para la instalación remota de la aplicación seleccionada en el asistente en Servidores de administración secundarios específicos.
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** → **Configuraciones específicas de Unix**.
4. Configure los siguientes ajustes:

- [Establecer una contraseña para la cuenta raíz \(solo para el despliegue a través de SSH\)](#) ⓘ

Si el comando `sudo` no se puede utilizar en el dispositivo de destino sin introducir la contraseña, seleccione esta opción y especifique la contraseña de la cuenta root. Kaspersky Security Center Linux transmite la contraseña en forma cifrada al dispositivo de destino, descifra la contraseña y luego inicia el procedimiento de instalación en nombre de la cuenta raíz con la contraseña especificada.

Kaspersky Security Center Linux no utiliza la cuenta ni la contraseña especificada para crear una conexión SSH.

- [Especifique la ruta a la carpeta temporal con permisos de ejecución en el dispositivo de destino \(solo para el despliegue a través de SSH\)](#) ⓘ



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 Linux utiliza el directorio especificado como directorio temporal para acceder 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.

## Reemplazo de aplicaciones de seguridad de terceros

La Instalación de aplicaciones de seguridad de Kaspersky a través de Kaspersky Security Center Linux puede requerir que se elimine el software de terceros incompatible con la aplicación instalada. Kaspersky Security Center Linux proporciona varias formas de eliminar las aplicaciones de terceros.

### Eliminar aplicaciones incompatibles al configurar la instalación remota de una aplicación

Puede habilitar la opción **Desinstalar automáticamente las aplicaciones incompatibles** al configurar la instalación remota de una aplicación de seguridad en el asistente de despliegue de la protección. Cuando esta opción se activa, Kaspersky Security Center Linux [elimina la aplicación incompatible antes de instalar una aplicación de seguridad en un dispositivo administrado](#).

### Eliminar aplicaciones incompatibles a través de una tarea dedicada

Para eliminar aplicaciones incompatibles, [use la tarea \*Desinstalar aplicación en remoto\*](#). 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 completar otra tarea** como tipo de programación, en el que la otra tarea es *Desinstalar aplicación en remoto*.

Este método de desinstalación es útil cuando el instalador de la aplicación de seguridad no puede eliminar correctamente una aplicación incompatible.

## Eliminación de aplicaciones o actualizaciones de software de forma remota

Puede eliminar aplicaciones o actualizaciones de software en dispositivos administrados que ejecutan Linux de forma remota solo mediante el Agente de red.

*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 **Añadir**.

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 Kaspersky Security Center.

4. En la lista **Tipo de tarea**, seleccione el tipo de tarea **Desinstalar aplicación en remoto**.

5. En el campo **Nombre de la tarea**, especifique el nombre de la tarea nueva.

El nombre de la tarea no puede tener más de 100 caracteres ni incluir caracteres especiales ("\*<>?\;|).

6. Seleccione los [dispositivos a los que se asignará la tarea](#).

Vaya al siguiente paso del asistente.

7. Seleccione qué tipo de software desea eliminar y luego seleccione aplicaciones, actualizaciones o parches específicos que desee eliminar:

- [Desinstalar aplicación administrada](#) ⓘ

Se muestra una lista de aplicaciones de Kaspersky. Seleccione la aplicación que desee eliminar.

- [Desinstalar 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 que se va a desinstalar** y, luego, seleccione la aplicación que desea eliminar.

b. Especifique las opciones de desinstalación:

- **Modo de desinstalación** 

Seleccione cómo desea eliminar la aplicación:

- **Definir comando de desinstalación automáticamente**

Si la aplicación tiene un comando de desinstalación definido por el proveedor de la aplicación, Kaspersky Security Center Linux usa este comando. Le recomendamos que seleccione esta opción.

- **Especificar 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 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:

**Usar este comando para desinstalación únicamente cuando el comando predeterminado no se detecte automáticamente** 

Kaspersky Security Center Linux 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 Linux lo usará en lugar del comando especificado en el campo **Comando para la desinstalación de la aplicación**.

Le recomendamos que habilite esta opción.

- **Reiniciar después de la desinstalación correcta de la aplicación** 

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 la actualización especificada de la aplicación, parche o aplicación de terceros** 

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](#).

8. Especifique cómo los dispositivos cliente descargarán la utilidad de desinstalación:

- [Usando 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 desactivada, los archivos se entregan mediante las herramientas del sistema operativo Linux.

Recomendamos habilitar esta opción cuando la tarea está asignada a dispositivos en los que se ha instalado el Agente de red.

- [Usando los recursos del sistema operativo mediante el Servidor de administración](#)

La opción está obsoleta. En su lugar, utilice la opción **Usando el Agente de red** o **Usando los recursos del sistema operativo mediante puntos de distribución**.

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.

- [Usando los recursos del sistema operativo mediante 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 **Usando 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.

- [Número máximo de descargas concurrentes](#)

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.

- [Número máximo de intentos de desinstalación](#) 

Si, al ejecutar la tarea *Desinstalar aplicación en remoto*, Kaspersky Security Center Linux no logra desinstalar una aplicación en un dispositivo administrado dentro del número de intentos de instalación especificado por el parámetro, Kaspersky Security Center Linux deja de enviar la utilidad de Desinstalación a este dispositivo administrado y ya no inicia el instalador en el dispositivo.

El parámetro **Número 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 **Número máximo de intentos de desinstalación** e iniciar la tarea para desinstalar la aplicación. Alternativamente, puede crear una nueva tarea *Desinstalar aplicación en remoto*.

- [Verificar el tipo de sistema operativo antes de descargar](#) 

Antes de transmitir los archivos a los dispositivos cliente, Kaspersky Security Center Linux verifica si la configuración de la utilidad de Instalación puede aplicarse al sistema operativo del dispositivo cliente. Si la configuración no puede aplicarse, Kaspersky Security Center Linux 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.

Vaya al siguiente paso del asistente.

9. 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 utilizando, 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 necesitan 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 manera predeterminada.

- **Repetir solicitud cada (min)**

- **Reiniciar después de (min)**

- **Forzar el cierre de las 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 manera predeterminada.

Vaya al siguiente paso del asistente.

10. Si es necesario, agregue las cuentas que se utilizarán para iniciar la tarea de desinstalación remota:

- **No es necesaria una cuenta (Agente de red 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 ha instalado en los dispositivos cliente.

- **Se necesita una cuenta (para la instalación sin 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*.

Indique qué cuenta se usará para ejecutar el instalador de la aplicación. Haga clic en el botón **Añadir**, seleccione **Cuenta** 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.

11. En el paso **Finalizar la creación de tareas** del asistente, active la opción **Abrir los detalles de la tarea cuando se complete la creación** para modificar la configuración de la tarea predeterminada.

Si no activa esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada más adelante.

12. Haga clic en el botón **Finalizar**.

El asistente crea la tarea. Si activó 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 especificar la configuración general de la tarea y, si es necesario, cambiar la configuración especificada durante la creación de la tarea.

También puede abrir la ventana de propiedades de la tarea si hace clic en el nombre de la tarea creada en la lista de tareas.

La tarea queda creada, configurada y se la muestra en la lista de tareas en **Activos (dispositivos) → Tareas**.

13. Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

También puede establecer una programación para el inicio de la tarea en la pestaña **Programación** de 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 aplicación seleccionada se desinstala de los dispositivos seleccionados.

## 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 verificar 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, Chef o puede crear su propio script; use cualquier método que le resulte conveniente.

Si el dispositivo no tiene las claves de firma GPG para SUSE Linux Enterprise, es posible que se encuentre con la siguiente advertencia: `Package header is not signed!` Seleccione la opción `i` para ignorar la advertencia.

Después de preparar el dispositivo SUSE Linux Enterprise Server 15, [implemente e instale el Agente de red](#).

## Preparar un dispositivo Windows para la instalación remota. Utilidad Riprep

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 **Desactivar 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 resolver los problemas que se han producido durante la instalación de la aplicación en un dispositivo cliente sin el Agente de red instalado, puede usar la utilidad diseñada para la preparación de los dispositivos para la instalación remota (riprep).

Use la utilidad riprep para preparar un dispositivo de Windows para la instalación remota. Para descargar la utilidad, haga clic en este enlace: <https://media.kaspersky.com/utilities/CorporateUtilities/KSC/riprep.exe>

La utilidad usada para preparar un dispositivo para la instalación remota no se puede ejecutar en Microsoft Windows XP Home Edition.

## Preparar un dispositivo Windows para la instalación remota en modo interactivo

*Para preparar un dispositivo Windows para la instalación remota en el modo interactivo:*



1. Ejecute el archivo riprep.exe en un dispositivo cliente.
2. En la ventana principal de la utilidad de preparación de la instalación remota, seleccione las siguientes opciones:
  - **Desactivar el uso compartido simple de archivos**
  - **Iniciar el servicio del Servidor de administración**
  - **Abrir puertos**
  - **Agregar una cuenta**
  - **Deshabilitar el Control de cuentas de usuario (UAC)** (disponible solo para dispositivos con Microsoft Windows Vista, Microsoft Windows 7 o Microsoft Windows Server 2008)

3. Haga clic en el botón **Iniciar**.

Las etapas de preparación del dispositivo para la instalación remota se muestran en la parte inferior de la ventana principal de la utilidad.

Si seleccionó **Agregar una cuenta**, cuando una cuenta se crea le solicitarán que escriba el nombre de la cuenta y la contraseña. Se creará una cuenta local, que pertenece al grupo de administradores locales.

Si seleccionó **Deshabilitar el Control de Cuentas de Usuario (UAC)**, se intentará deshabilitar el Control de Cuentas de Usuario incluso si ya se lo deshabilitó antes de iniciar la utilidad. Después de que UAC se deshabilite, le solicitarán reiniciar el dispositivo.

## Preparar un dispositivo Windows para la instalación remota en modo silencioso

*Para preparar un dispositivo Windows para la instalación remota en el modo no interactivo:*

Ejecute el archivo riprep.exe en el dispositivo cliente desde la línea de comandos con el conjunto de claves requerido.

Sintaxis de línea de comandos de la utilidad:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Descripciones de las claves:

- **-silent**: ejecutar la utilidad en modo no interactivo.
- **-cfg CONFIG\_FILE**: define la configuración de la utilidad, donde CONFIG\_FILE es la ruta al archivo de configuración (un archivo con la extensión .ini).
- **-tl traceLevel**: define el nivel de seguimiento donde traceLevel es un número de 0 a 5. Si no se especifica una clave, se usa el valor 0.

Si inicia la utilidad en modo silencioso, podrá realizar las siguientes tareas:

- **Deshabilitar el uso compartido simple de archivos**

- Iniciar el servicio del servidor en el dispositivo cliente
- Abrir los puertos
- Crear una cuenta local
- Deshabilitar el Control de cuentas de usuario (UAC)

Puede indicar los parámetros de preparación del dispositivo para la instalación remota en el archivo de configuración especificado en la clave `-cfg`. Para definir estos parámetros, agregue la siguiente información al archivo de configuración:

- En la sección `Common` especifique las tareas que se deben ejecutar:
  - `DisableSFS`: deshabilitar el uso compartido de archivos (0: la tarea está deshabilitada; 1: la tarea está habilitada).
  - `StartServer`: inicia el servicio del servidor (0: la tarea está deshabilitada; 1: la tarea está habilitada).
  - `OpenFirewallPorts`: abre los puertos necesarios (0: la tarea está deshabilitada; 1: la tarea está habilitada).
  - `DisableUAC`: deshabilita el Control de cuentas de usuario (UAC) (0: la tarea está deshabilitada; 1: la tarea está habilitada).
  - `RebootType`: define el comportamiento que se debe seguir si se requiere reiniciar el dispositivo cuando se deshabilita el UAC. Puede utilizar los siguientes parámetros:
    - 0: Nunca reiniciar el dispositivo.
    - 1: Reiniciar el dispositivo, si UAC se habilitó antes de iniciar la utilidad.
    - 2: Forzar el reinicio, si UAC se habilitara antes de iniciar la utilidad.
    - 4: Siempre reiniciar el dispositivo.
    - 5: Siempre reiniciar el dispositivo de manera forzada.
- En la sección `UserAccount` especifique el nombre de la cuenta (`user`) y su contraseña (`Pwd`).

Contexto de muestra del archivo de configuración:

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1
[UserAccount]
user=Admin
Pwd=Pass123
```

Después de que se completa la utilidad, se crearán los siguientes archivos en la carpeta de inicio de la utilidad:

- `riprep.txt`: informe de operaciones, en el cual las fases del funcionamiento de la utilidad se enumeran con motivos para las operaciones.
- `riprep.log`: archivo de seguimiento (se crea si el nivel de seguimiento es superior a 0).

# Licencias

Esta sección proporciona la siguiente información:

- Conceptos generales relacionados con las licencias de Kaspersky Security Center Linux
- Instrucciones sobre la administración de licencias de aplicaciones de Kaspersky administradas

## Acerca de las licencias de Kaspersky Security Center Linux

Esta sección describe los conceptos generales relacionados con la licencia de Kaspersky Security Center Linux.

## 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 Linux y sus componentes, por ejemplo, el Agente de red, tienen su propio EULA.

Puede ver las condiciones del Contrato de licencia de usuario final para Kaspersky Security Center Linux 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 las condiciones del Contrato de licencia de usuario final para Agente de red para Linux utilizando los siguientes métodos:

- Mientras se descarga de paquete de distribución del Agente de red desde los servidores web de Kaspersky.
- Durante la instalación del Agente de red para Linux.
- Leyendo el documento license.txt incluido en el paquete de distribución del Agente de red para Linux.
- Leyendo el documento license.txt en la carpeta de instalación de 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 de la licencia

Una *licencia* otorga el derecho a usar Kaspersky Security Center Linux 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 ofrecen los siguientes tipos de licencia:

- *De prueba*

Se trata de una licencia gratuita, que puede utilizarse para probar la aplicación. Usualmente, una licencia de prueba tiene un plazo de vigencia breve.

Al caducar la licencia de prueba, se desactivan todas las funciones de Kaspersky Security Center Linux. 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 desactivan 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 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 otorgada:

- Clave de licencia o número de pedido
- 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.

## Ver la Política de privacidad

La Política de privacidad está disponible en línea en <https://www.kaspersky.es/products-and-services-privacy-policy>.

La Política de privacidad también está disponible sin conexión:

- Puede leer la Política de privacidad antes de [instalar Kaspersky Security Center Linux](#).
- El texto de la Política de privacidad se incluye en el archivo `license.txt`, en la carpeta de instalación de Kaspersky Security Center Linux.
- El archivo `privacy_policy.txt` está disponible en un dispositivo administrado, en la carpeta de instalación del Agente de red.
- Puede desempaquetar el archivo `privacy_policy.txt` desde el paquete de distribución del Agente de red.

## Opciones de licencias de Kaspersky Security Center

Kaspersky Security Center se entrega como parte de las aplicaciones de Kaspersky para la protección de redes corporativas. También se puede descargar desde el [sitio web de Kaspersky](#).

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.
- Realice la instalación remota de aplicaciones de Kaspersky y otros proveedores de software.
- 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.
- Administre el cifrado de la información almacenada en los discos duros de los dispositivos basados en Windows y las unidades extraíbles.
- Administre el acceso de los usuarios a los datos cifrados en dispositivos basados en Windows.
- 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.

## 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.

## Sobre la provisión de datos

### Datos procesados localmente

Kaspersky Security Center Linux está diseñado para la ejecución centralizada de las tareas básicas de administración y de mantenimiento en la red de una organización. Kaspersky Security Center Linux proporciona al administrador acceso a información detallada sobre el nivel de seguridad de la red de la organización; Kaspersky Security Center Linux le permite al administrador configurar todos los componentes de protección de las aplicaciones de Kaspersky. Kaspersky Security Center Linux realiza las siguientes funciones principales:

- 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
- 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 realizar sus principales funciones, Kaspersky Security Center Linux puede recibir, almacenar y procesar la siguiente información:

- Información sobre los dispositivos en la red de la organización recibida mediante el análisis de los controladores de dominio Active Directory o Samba, o mediante el análisis de los intervalos de IP. El Servidor de administración recaba datos de forma independiente o recibe información del Agente de red.
- Información de Active Directory y Samba sobre unidades organizativas, dominios, usuarios y grupos. El Servidor de administración obtiene datos por sí mismo o recibe datos del Agente de red asignado para funcionar 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 introduce el nombre para mostrar y la descripción del dispositivo en la interfaz de Kaspersky Security Center Web Console:
  - Especificaciones técnicas del dispositivo administrado y de sus componentes necesarias para identificar el dispositivo: nombre y descripción del dispositivo; nombre y tipo de dominio de Windows (para dispositivos que pertenecen a un dominio de Windows); nombre del dispositivo en el entorno de Windows (para dispositivos que pertenecen a un dominio de Windows); dominio DNS y nombre DNS; dirección IPv4; dirección IPv6; ubicación de red; dirección MAC; tipo de sistema operativo; indicación de si el dispositivo es una máquina virtual y tipo de hipervisor; indicación de si el dispositivo es una máquina virtual dinámica que forma parte de una VDI.
  - Otras especificaciones de dispositivos administrados y sus componentes necesarios para la auditoría de dispositivos administrados: 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.
  - 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 Kaspersky Security Center Web Console.
- 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 protección en tiempo real, fecha y hora del último análisis del dispositivo, número de amenazas detectadas, número de objetos que no se desinfectaron, disponibilidad y estado del componentes de la aplicación, detalles de las configuraciones y tareas de la aplicación Kaspersky, información sobre las claves de licencia activas y de reserva, fecha de instalación e id. 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.
- Datos contenidos en los eventos de los componentes de Kaspersky Security Center Linux y las aplicaciones de Kaspersky administradas. El Agente de red transfiere datos del dispositivo al Servidor de administración.
- Configuración de los componentes de Kaspersky Security Center Linux y las aplicaciones administradas de Kaspersky presentadas en las directivas y los perfiles de las directivas El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- Configuración de las tareas de los componentes de Kaspersky Security Center Linux y las aplicaciones administradas de Kaspersky El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- Datos procesados por la función de administración del Sistema. El Agente de red transfiere la siguiente información del dispositivo al Servidor de administración:
  - Información sobre el hardware detectado en los dispositivos administrados (Registro de hardware).
  - Información sobre el software instalado en los dispositivos administrados (registro de software). El software se puede comparar con la información sobre los archivos ejecutables detectados en los dispositivos por la función Control de aplicaciones.
- Categorías de aplicaciones creadas por el usuario. El usuario ingresa datos 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. 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 dispositivos basados en Windows 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 en dispositivos basados en Windows realizados con 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.
- 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.
- 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. Una aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red.
- Información sobre los errores de cifrado de datos en los dispositivos: El cifrado lo realiza la función de cifrado de datos de las aplicaciones de Kaspersky. Una aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. La lista completa de datos se proporciona en los archivos de la Ayuda en línea 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.
- Detalles de los códigos de activación y archivos clave introducidos. 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 y contraseña. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- Historial de revisiones de los objetos de administración. El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- Registro de objetos de administración eliminados. El usuario ingresa datos 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 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.
- Certificado para la conexión segura de dispositivos administrados a los componentes de Kaspersky Security Center Linux El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- Información sobre qué términos del acuerdo legal de Kaspersky ha aceptado el usuario.
- Los datos del Servidor de administración que el Usuario introduce en Kaspersky Security Center Web Console o en la interfaz del programa Kaspersky Security Center Open API.
- Cualquier dato que el Usuario introduzca en la interfaz de Kaspersky Security Center Web Console.

Los datos enumerados anteriormente pueden estar presentes en Kaspersky Security Center Linux si se aplica uno de los siguientes métodos:

- El usuario ingresa datos en la interfaz de Kaspersky Security Center Web Console.
- 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 acerca de los dispositivos conectados a una red por sí mismo o recibe datos del Agente de red asignado para funcionar como punto de distribución.

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 procesados de forma local solo pueden transferirse a Kaspersky a través de archivos de volcado, archivos de seguimiento o archivos de registro de componentes de Kaspersky Security Center Linux, entre ellos archivos de registro creados por instaladores y utilidades.

Los archivos de volcado, los archivos de seguimiento o los archivos de registro de los componentes de Kaspersky Security Center Linux contienen datos arbitrarios del Servidor de administración, el Agente de red y Kaspersky Security Center Web Console. Los archivos pueden contener datos personales o confidenciales. Los archivos de volcado, los archivos de seguimiento o los archivos de registro se almacenan en los dispositivos sin cifrar. Los archivos de volcado, los archivos de seguimiento o los archivos de registro no se transfieren automáticamente a Kaspersky; sin embargo, un administrador puede transferir esos archivos a Kaspersky manualmente si así lo solicita el servicio de Soporte técnico para resolver problemas relacionados con el funcionamiento de Kaspersky Security Center Linux.

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.

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 Linux.

- Versión de Kaspersky Security Center Linux.
- Localización de Kaspersky Security Center Linux.
- 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.

## Acerca de la suscripción

Una *Suscripción a Kaspersky Security Center Linux* es una solicitud para usar la aplicación con las opciones seleccionadas (fecha de vencimiento de la suscripción, cantidad de dispositivos protegidos). Puede registrar la suscripción a Kaspersky Security Center Linux 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 utilizar Kaspersky Security Center Linux con suscripción, debe aplicar el código de activación facilitado por el proveedor de servicios.

Puede aplicar otro código de activación para Kaspersky Security Center Linux solo cuando caducado la suscripción caduque o usted la cancele.

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.

Cuando la aplicación se utiliza bajo suscripción, Kaspersky Security Center Linux intenta acceder automáticamente al servidor de activación a intervalos de tiempo especificados, hasta que caduque la suscripción. Si no es posible acceder al servidor mediante el DNS del sistema, la aplicación utiliza [servidores DNS públicos](#). Si necesita renovar su suscripción, puede hacerlo en el sitio web de su proveedor de servicios.

## Activación de Kaspersky Security Center Linux

Puede activar las características de la licencia para utilizar las funciones adicionales de Kaspersky Security Center Linux. Existen dos formas para realizar esta tarea: utilizar el [Asistente de inicio rápido del Servidor de administración](#) o las propiedades del Servidor de administración.

*Para activar características de licencia de Kaspersky Security Center Linux, 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 **General**, vaya a la sección **Claves de licencia**.
3. En **Licencia actual**, haga clic en el botón **Seleccionar**.
4. En la ventana que se abre, elija la clave de licencia que desee usar para activar Kaspersky Security Center Linux. Si la clave de licencia no aparece en la lista, haga clic en el botón **Añadir una nueva clave de licencia** y, luego, especifique una nueva clave de licencia.
5. Si es necesario, también puede añadir una [clave de licencia de reserva](#) 📄. Para hacerlo, en **Clave de licencia de reserva**, haga clic en el botón **Seleccionar** y, luego, elija una clave de licencia existente o añada una nueva. Tenga en cuenta que no puede añadir una clave de licencia de reserva si no hay una clave de licencia activa.
6. Haga clic en el botón **Guardar**.

## Licencias de aplicaciones de Kaspersky administradas

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 Linux le permite realizar una distribución centralizada de las claves de licencia para las aplicaciones 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 activado la opción **Clave de licencia distribuida automáticamente** para las tres claves de licencia. En los dispositivos de la organización se ha instalado una aplicación de seguridad de Kaspersky, por ejemplo, Kaspersky Endpoint Security for Linux. 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:

- [Agregar una clave de licencia al repositorio del Servidor de administración](#)
- [Distribución automática de una clave de licencia](#)

Tenga en cuenta que es posible que una clave de licencia distribuida automáticamente no se muestre 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 dispositivos administrados.
- La clave de licencia ya se ha utilizado para dispositivos administrados por otro Servidor de administración virtual y se ha alcanzado el límite del número 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: [añadir 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:

- [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 **Añadir**.

3. Elija lo que quiera agregar:

- **Añadir archivo clave**

Haga clic en el botón **Seleccionar archivo clave** y vaya al archivo de clave que desea agregar.

- **Introducir el 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.

## 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 añadir clave.

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 a través de la tarea de añadir clave, siga estos pasos:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Añadir**.  
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 añadir una clave de licencia.
4. En la lista **Tipo de tarea**, seleccione la tarea **Añadir clave**.
5. En el campo **Nombre de la tarea**, especifique el nombre de la tarea nueva.
6. Seleccione los [dispositivos a los que se asignará la tarea](#).
7. En el paso **Selección de una clave de licencia** del asistente, haga clic en el enlace **Añadir clave** para añadir la clave de licencia.
8. En el panel de adición de claves, añada la clave de licencia mediante una de las siguientes opciones:

Debe añadir la clave de licencia solo si no la añadió al repositorio del Servidor de administración antes de crear la tarea de añadir clave.

- Seleccione la opción **Introducir el código de activación** para introducir 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 de adición de claves.
  - b. Haga clic en el botón **Guardar**.

Si desea distribuir la clave de licencia a los dispositivos administrados automáticamente, active la opción **Distribuir automáticamente la clave de licencia a los dispositivos administrados**.

Se cierra el panel de adición de claves.

- Seleccione la opción **Añadir archivo clave** para añadir un archivo de clave y luego haga lo siguiente:
  - a. Haga clic en el botón **Seleccionar archivo 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 aparece en el panel de adición de clave de licencia.
  - c. Haga clic en el botón **Guardar**.

Si desea distribuir la clave de licencia a los dispositivos administrados automáticamente, active la opción **Distribuir automáticamente la clave de licencia a los dispositivos administrados**.

Se cierra el panel de adición de claves.

9. Seleccione la clave de licencia en la tabla de claves.

10. En el paso **Información de licencia** del asistente, active la opción **Usar como clave de reserva** si desea usar esta clave como clave de reserva.

En este caso, se aplica una clave de reserva cuando caduca la clave activa.

11. En el paso **Finalizar la creación de tareas** del asistente, active la opción **Abrir los detalles de la tarea cuando se complete la creación** para modificar la configuración de la tarea predeterminada.

Si no activa esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada más adelante.

12. Haga clic en el botón **Finalizar**.

El asistente crea la tarea. Si activó 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 especificar la [configuración general de la tarea](#) y, si es necesario, cambiar la configuración especificada durante la creación de la tarea.

También puede abrir la ventana de propiedades de la tarea si hace clic en el nombre de la tarea creada en la lista de tareas.

Se crea la tarea, se la configura y se la muestra 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 establecer una programación para el inicio de la tarea en la pestaña **Programación** de 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 Linux permite la distribución automática de claves de licencias en dispositivos administrados si estas se encuentran en el repositorio de claves 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 automáticamente la clave de licencia a los dispositivos administrados**.



4. Haga clic en el botón **Guardar**.

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 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 es posible que una clave de licencia distribuida automáticamente no se muestre 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 dispositivos administrados.
- La clave de licencia ya se ha utilizado para dispositivos administrados por otro Servidor de administración virtual y se ha alcanzado el límite del número de dispositivos.

Si selecciona la casilla de verificación **Distribuir automáticamente la clave de licencia 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.

## 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 no es posible acceder a los servidores mediante el DNS del sistema, la aplicación utiliza [servidores de DNS públicos](#).

## Eventos sobre límites de licencia superados

Kaspersky Security Center Linux permite obtener información sobre los eventos que ocurren cuando el Servidor de administración y otras aplicaciones Kaspersky instaladas en dispositivos cliente exceden determinados límites de licencias.

El nivel de importancia de estos eventos se define sobre la base de estas 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**.

## Eliminar una clave de licencia del repositorio

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. Compruebe que el Servidor de administración no utilice un archivo clave o un código de activación que desea eliminar. Si el Servidor de administración lo hace, no puede eliminar la clave. Para realizar la comprobación:
  - a. En el menú principal, haga clic en el ícono de configuración (⚙️) junto al nombre del Servidor de administración.  
Se abre la ventana Propiedades del Servidor de administración.
  - b. En la pestaña **General**, vaya a la sección **Claves de licencia**.

c. Si la clave de licencia o código de activación requeridos aparecen en la sección que se abre, haga clic en el botón **Eliminar clave de licencia activa** y luego confirme la operación. Después de eso, el Servidor de administración no usa la clave de licencia eliminada, pero la clave permanece en el repositorio del Servidor de administración. Si el archivo clave o el código de activación requeridos no aparecen, el Servidor de administración no los utiliza.

2. En el menú principal, vaya a **Operaciones** → **Licencias** → **Licencias de Kaspersky**.

3. Seleccione el archivo clave o el código de activación requeridos y luego 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.

*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 una de las siguientes acciones:

- En el menú principal, vaya a **Operaciones** → **Licencias** → **Licencias de Kaspersky**.
- En el menú principal, vaya a **Control 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 Linux: la versión, la localización que está utilizando, el ID de la licencia de 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

**Mercado** 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 Linux le 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 **Mercado**:

- 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, por sus siglas en inglés). En este nivel, las empresas necesitan soluciones que les permitan contrarrestar amenazas complejas y ataques dirigidos.
- Tipos de activos que desea proteger:
  - **Puntos finales**: estaciones de trabajo de 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
  - **Servicio**: servicios relacionados con la seguridad proporcionados por Kaspersky

*Para buscar y comprar una solución empresarial de Kaspersky:*

1. En el menú principal, vaya a **Mercado**.

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.

# Configuración de las aplicaciones de Kaspersky

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.

## Escenario: 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 inadmisibles para su organización. Por este motivo, recomendamos que modifique estas directivas y tareas, y que cree otras directivas y tareas para su red de ser necesario.

### Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

- [Instalado el Servidor de administración de Kaspersky Security Center Linux](#)
- [Instaló Kaspersky Security Center Web Console](#)
- Completado el escenario de instalación principal de Kaspersky Security Center Linux
- Completado el [asistente de inicio rápido](#) o creado manualmente las siguientes directivas y tareas en el grupo de administración de **Dispositivos administrados**:
  - Directiva de Kaspersky Endpoint Security
  - Tarea de grupo para actualizar Kaspersky Endpoint Security
  - Directiva del Agente de red

### Etapas

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 se pueden combinar.

#### 2 Configurar tareas para administrar las aplicaciones de Kaspersky en forma remota

Verifique las tareas creadas con el asistente de inicio rápido y ajústelas, si es necesario.

Instrucciones: [Configuración de la tarea de grupo para actualizar Kaspersky Endpoint Security](#).

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

Cuando ocurre un evento en una aplicación administrada, el dispositivo cliente en el que tuvo lugar el suceso transfiere información al respecto a 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 prácticas: [Configurar el 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](#).

## 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.

La [administración de seguridad centrada en el dispositivo](#) le permite aplicar distintas configuraciones de la aplicación de seguridad a los dispositivos administrados según las funciones específicas del dispositivo. Es posible, por ejemplo, definir ajustes de configuración diferentes para dispositivos asignados a grupos de administración diferentes.

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 el Servidor de administración de Kaspersky Security Center Linux](#) y [Kaspersky Security Center Web Console](#). También es posible que desee considerar la [administración de seguridad centrada en el usuario](#) como una opción alternativa o adicional al enfoque centrado en el dispositivo. Más información sobre [dos enfoques de administración](#).

### 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 configura la protección de su red en el asistente de inicio rápido, Kaspersky Security Center Linux crea la directiva predeterminada para las siguientes aplicaciones:

- Kaspersky Endpoint Security for Linux (para dispositivos cliente con Linux)
- Kaspersky Endpoint Security para Windows (para dispositivos cliente con Windows)

Si completó el proceso de configuración utilizando este asistente, no tiene que crear una nueva directiva para esta aplicación.

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 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.

Al utilizar las condiciones de activación del perfil, puede aplicar diferentes perfiles de directivas, por ejemplo, a los dispositivos que tienen configuración de hardware específica o marcados con [etiquetas](#) específicas. Puede usar las etiquetas para filtrar dispositivos que reúnen criterios específicos. Por ejemplo, puede crear una etiqueta llamada *CentOS*, marcar todos los dispositivos que ejecutan el sistema operativo CentOS con esta etiqueta y luego especificar esta etiqueta como condición de activación para un perfil de directiva. Como resultado, las aplicaciones de Kaspersky instaladas en todos los dispositivos que ejecutan CentOS serán administradas por su propio perfil de directiva.

Instrucciones:

- [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. Las directivas nuevas o con cambios y los perfiles de directivas se propagan a los dispositivos administrados durante la sincronización. Puede saltar 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 Linux 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.

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.

## Requisitos previos

Antes de comenzar, asegúrese de haber instalado correctamente [el Servidor de administración de Kaspersky Security Center Linux](#) y [Kaspersky Security Center Web Console](#) y de haber completado el escenario de despliegue principal. También es posible que desee considerar la [administración de seguridad centrada en el dispositivo](#) como una opción alternativa o adicional al 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 Linux crea la directiva predeterminada para Kaspersky Endpoint Security. Si completó el proceso de configuración utilizando este asistente, no tiene que crear una nueva directiva para esta aplicación.

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, Kaspersky Security Center Linux sincroniza automáticamente el Servidor de administración 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 saltar 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 Linux 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.

## 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 ajustes de aplicaciones de Kaspersky que se aplican a 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 política tiene uno de los siguientes estados:

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.
- 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 produce 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                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  Undefined <input type="checkbox"/>          | 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 <i>desbloqueados</i> . |
|  Enforce <input checked="" type="checkbox"/> | 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:

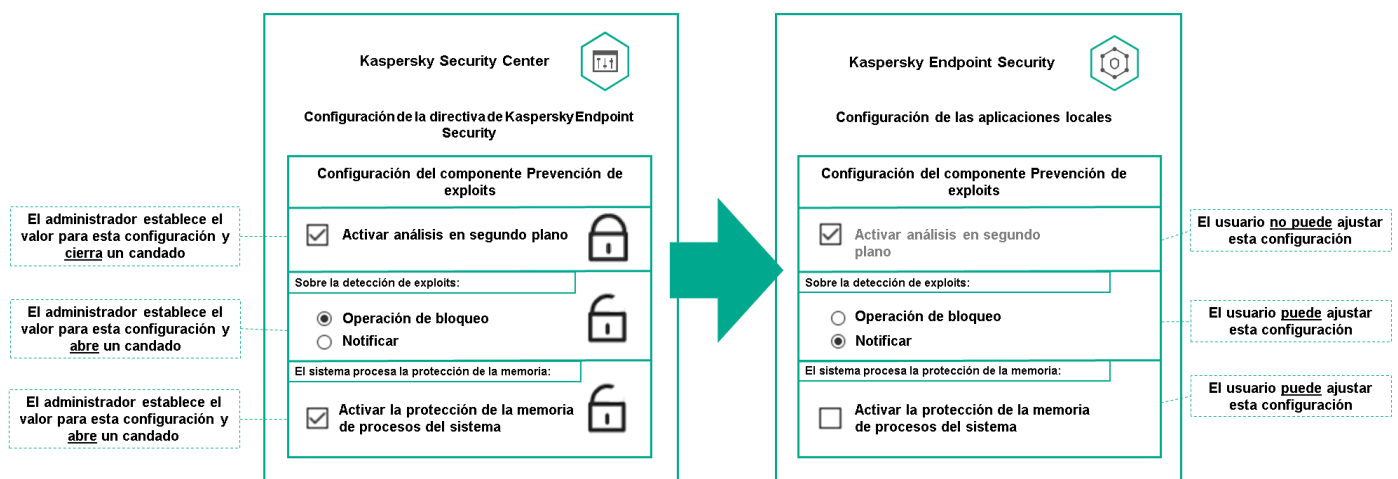
- Bloquear ajustes en la directiva de un subgrupo de administración
- Bloquear los ajustes de una aplicación de Kaspersky instalada en un dispositivo administrado

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

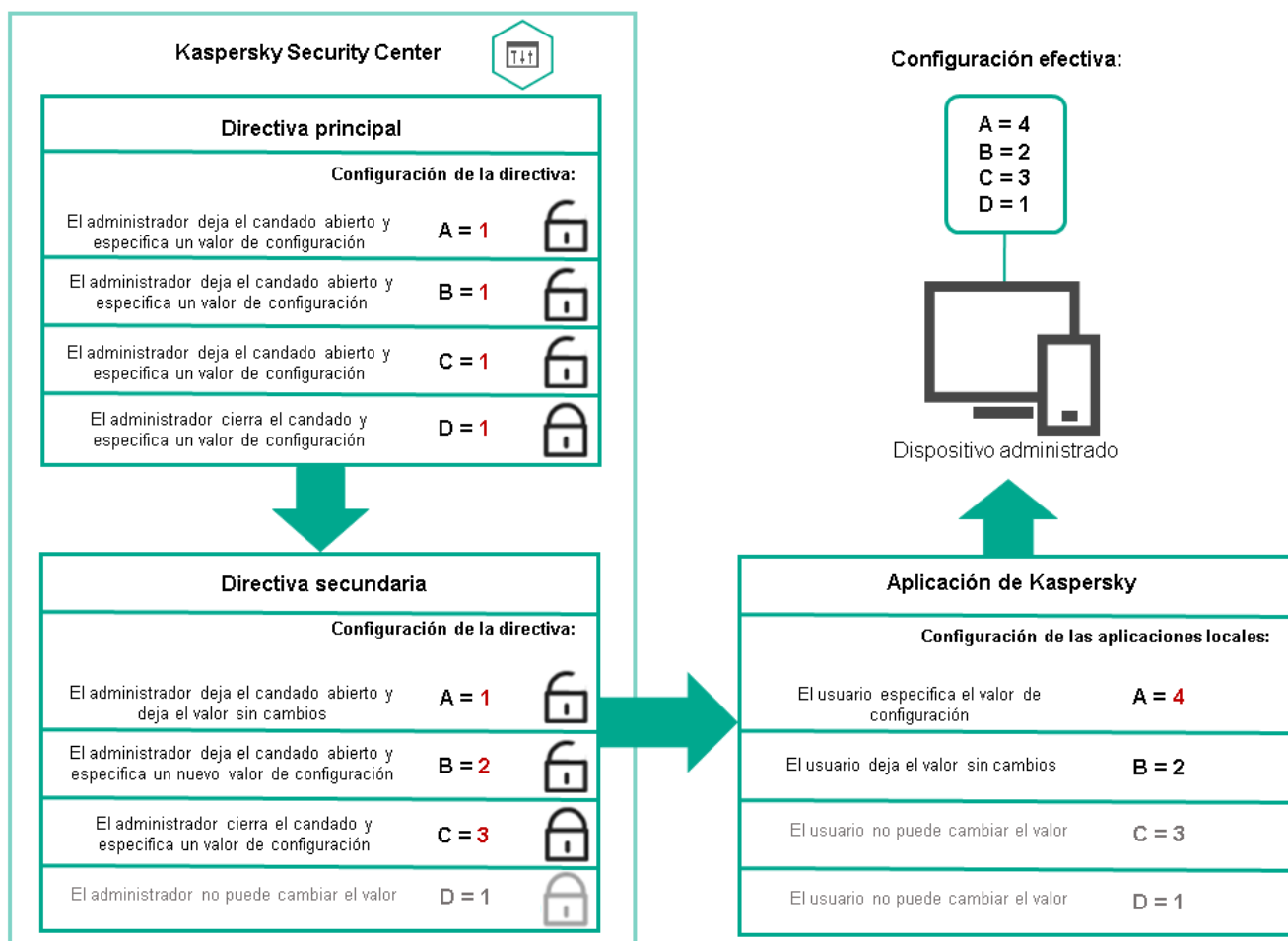
Si distintos dispositivos necesitan diferentes configuraciones, puede organizar los dispositivos en grupos de administración.

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).

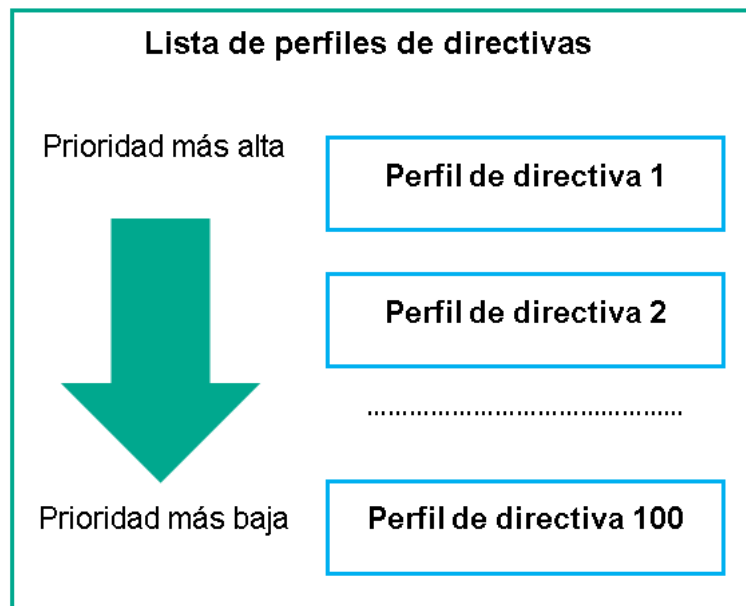


Jerarquía de directivas

## Perfiles de directivas en una jerarquía de directivas

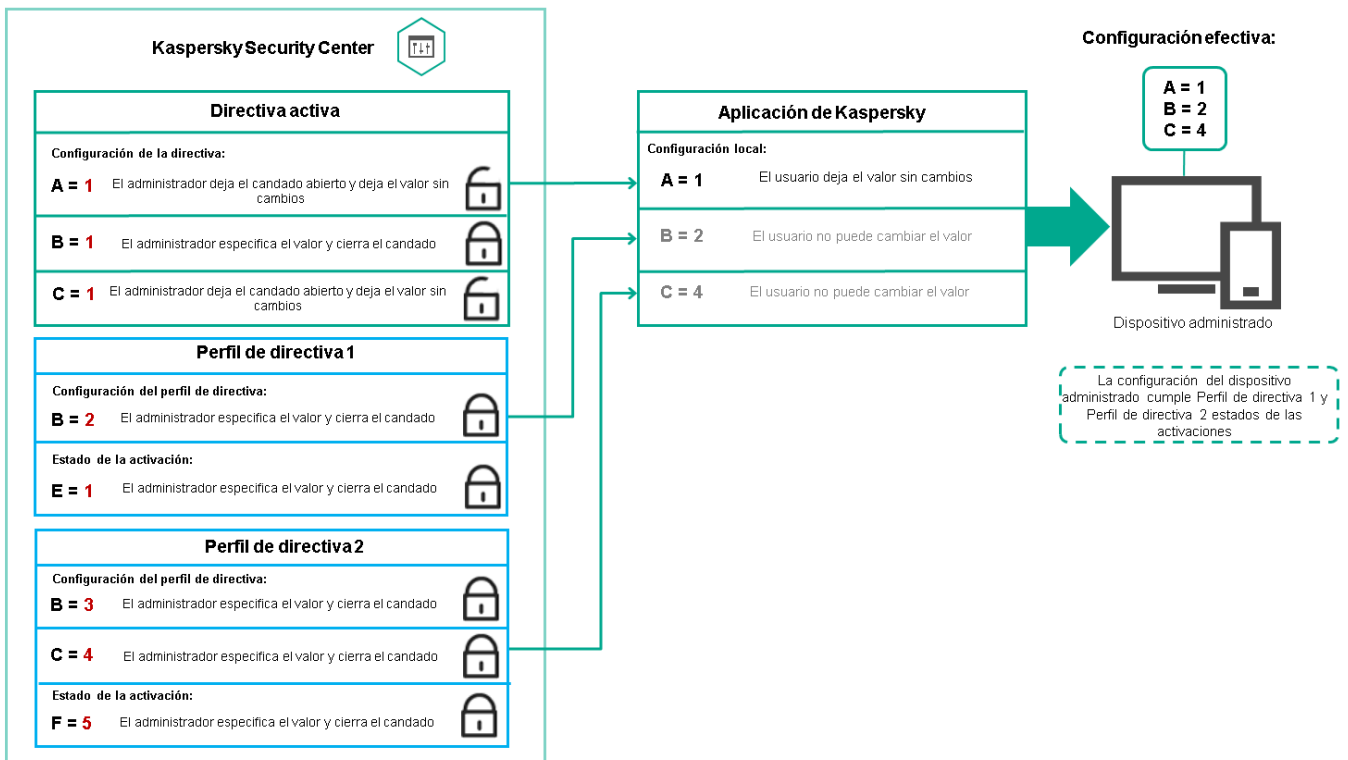
Los perfiles de directivas tienen las siguientes condiciones de asignación de prioridad:

- 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).



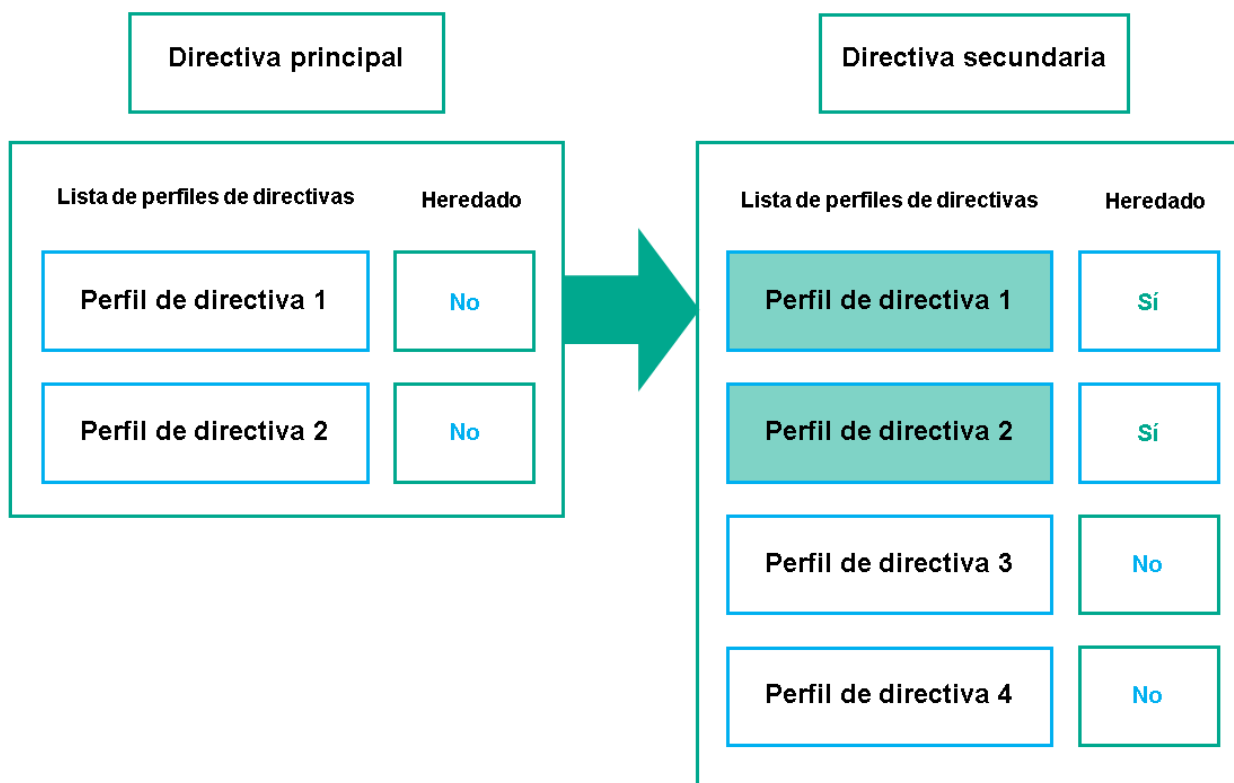
La configuración del dispositivo administrado cumple las condiciones de activación de varios perfiles de directiva

## 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).

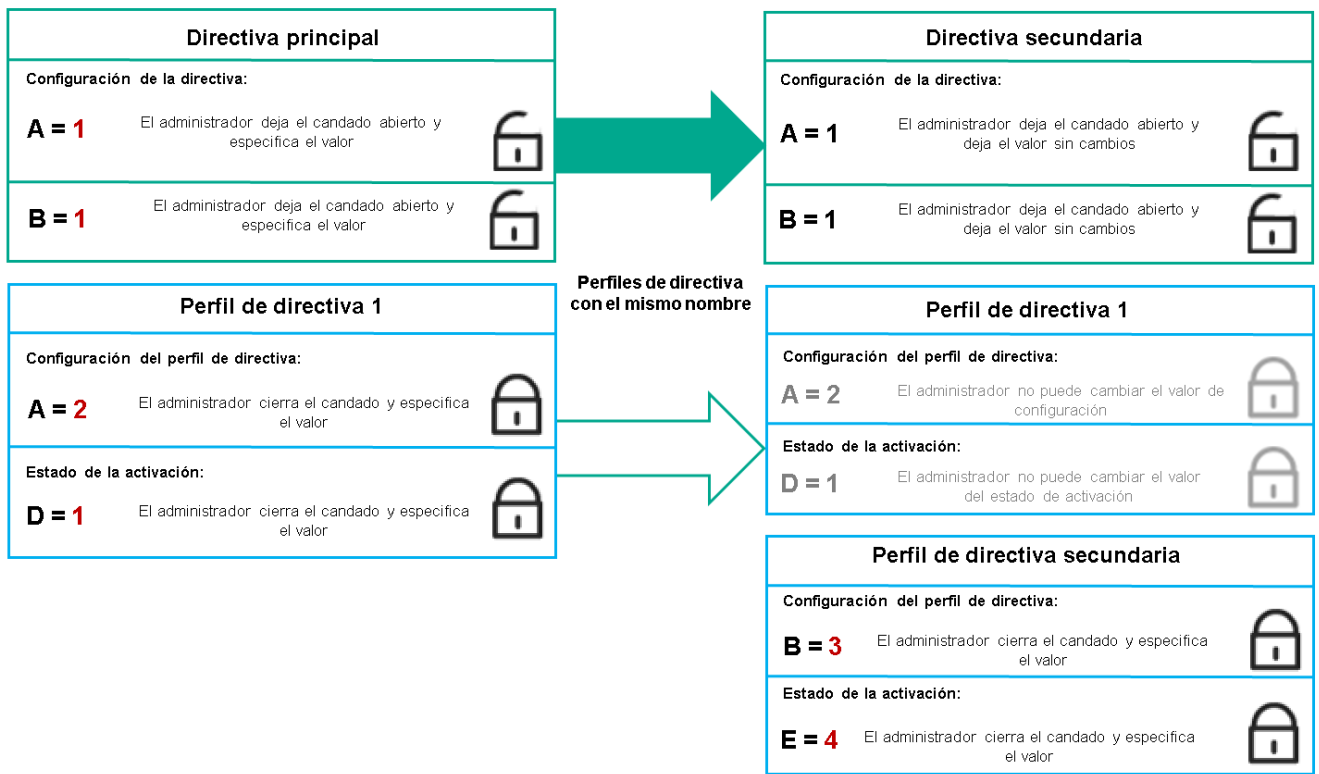


Herencia de perfiles de directivas

## 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. Haga clic en **Añadir**.  
Se abre la ventana **Seleccionar aplicación**.
3. Seleccione la aplicación para la que desee crear la directiva.
4. Haga clic en **Siguiente**.  
Se abre la ventana de configuración de la nueva directiva, con la pestaña **General** seleccionada.
5. Si lo desea, cambie el nombre predeterminado, el estado predeterminado y las opciones de directiva predeterminadas.
6. 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.
7. 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](#)

- [Ayuda de Kaspersky Endpoint Security for Linux](#) <sup>?</sup>
- [Ayuda de Kaspersky Endpoint Security para Windows](#) <sup>?</sup>

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.

8. Haga clic en **Guardar** para guardar la directiva.

La directiva aparecerá en la lista de directivas.

## 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](#) <sup>?</sup>

Si se selecciona esta opción, se activa la directiva.  
Esta opción está seleccionada de manera predeterminada.

- [Fuera de la oficina](#) <sup>?</sup>

Una directiva “fuera de la oficina” entra en vigor (es decir, se activa) cuando el dispositivo sale de la red corporativa.

- [Inactiva](#) <sup>?</sup>

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](#) <sup>?</sup>

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 habilitada de manera predeterminada.

- [Forzar la herencia de la configuración en las directivas secundarias](#) <sup>?</sup>

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 manera 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.

- **Fallo operativo**

- **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 eventos**

Puede especificar cuántos días se conservará el evento y dónde se lo guardará:

- **Exportar al sistema SIEM a través de Syslog**
- **Almacenar en el registro de eventos del SO del dispositivo**
- **Almacenar en el registro de eventos del SO del Servidor de administración**

- **Notificaciones de 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 script o archivo ejecutable**
- **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 lanzar**.

## Historial de revisión

La pestaña **Historial de revisión** le permite ver la lista de revisiones de la directiva y [revertir los cambios](#) realizados en la directiva, si es necesario.

## 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](#)
  - [Ayuda de Kaspersky Endpoint Security for Linux](#) <sup>🔗</sup>
  - [Ayuda de Kaspersky Endpoint Security para Windows](#) <sup>🔗</sup>

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 revisión**.

## 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 la 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 Linux le permite guardar una directiva, su configuración y los perfiles de la directiva en un archivo KLP. Puede utilizar este archivo KLP para [importar la directiva guardada](#) tanto para Kaspersky Security Center Windows como para Kaspersky Security Center Linux.

*Para exportar una directiva:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.

2. Marque la casilla que hay junto a la directiva que desea exportar.

No puede exportar varias directivas al mismo tiempo. Si selecciona más de una directiva, el botón **Exportar** se desactivará.

3. Haga clic en el botón **Exportar**.

4. En la ventana **Guardar como** abierta, especifique la ruta y el nombre del archivo de la directiva. Haga clic en el botón **Guardar**.

La ventana **Guardar como** se muestra solo si usa Google Chrome, Microsoft Edge u Opera. Si utiliza otro navegador, el archivo de la directiva se guarda automáticamente en la carpeta **Descargas**.

## Importación de una directiva

Kaspersky Security Center Linux le permite importar una directiva desde un archivo KLP. El archivo KLP contiene la [directiva exportada](#), su configuración y los perfiles de directiva.

*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 abierta, especifique la ruta al archivo de directiva de KLP y, a continuación, haga clic en el botón **Abrir**. Tenga en cuenta que solo puede seleccionar un archivo de directiva.  
Se inicia el procesamiento de la directiva.
5. Después de que la directiva se procese correctamente, seleccione el grupo de administración al que desea aplicar la directiva.
6. Haga clic en el botón **Completar** para finalizar la importación de políticas.

Aparece la 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.

Después de una importación correcta, la directiva aparece 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)**.

## Sincronización forzada

Si bien Kaspersky Security Center Linux sincroniza el estado, la configuración, las tareas y las directivas para los dispositivos administrados automáticamente, en algunos casos, usted debe saber exactamente si la sincronización ya se ha realizado para un dispositivo específico en un momento dado.

### 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. Haga clic en 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.

## Ver el gráfico de distribución de una directiva

En Kaspersky Security Center Linux, puede ver el estado de la aplicación de directivas en cada dispositivo en un gráfico del estado de distribución de directivas.

*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. La lista puede mostrar un máximo de 100 000 dispositivos.

*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, elija **Opciones de interfaz**.
2. En el campo **Límite de dispositivos que se incluirán en los resultados de distribución de las directivas**, indique un número de dispositivos (con un máximo de 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 describe la gestión de perfiles de directivas y proporciona información sobre cómo ver los perfiles de una directiva, cambiar la prioridad de un perfil de directiva, crear un perfil de directiva, copiar un perfil de directiva, crear una regla de activación de perfil de directiva y eliminar 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 **Despriorizar**.

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 **Añadir**.

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.

## 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 **Añadir**.

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 de activación de perfiles de directivas](#) 

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.
- **Desconectado:** 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.

- [La regla de conexión con el 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 manera predeterminada.

- [El propietario del dispositivo está incluido en un grupo de seguridad interno](#) 

Seleccione esta opción para configurar y activar la regla de activación de perfil en el dispositivo según la pertenencia del propietario del dispositivo a un grupo interno de seguridad de Kaspersky Security Center Linux. 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. Puede especificar un grupo de seguridad de Kaspersky Security Center Linux. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de manera predeterminada.

- **[Reglas para especificaciones de 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 manera 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 manera predeterminada.

- **Reglas para la asignación de funciones**

Si elige esta opción, defina esto en el paso siguiente:

- [Activar perfil de directiva según la función específica 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 etiquetas](#) 

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:

- [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 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 manera predeterminada.

El número de páginas adicionales del asistente depende de la configuración que seleccione 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.

## 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. La ventana de propiedades contiene las pestañas y los ajustes que se describen a continuación.

Tenga en cuenta que para dispositivos basados en Linux y Windows, hay [varias configuraciones](#) disponibles.

### General

En la pestaña, puede modificar el estado de la directiva y especificar cómo se heredarán los ajustes 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 manera predeterminada.

- [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 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 habilitada de manera predeterminada.

- [Forzar la herencia de la 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 manera predeterminada.

## Configuración de eventos

En esta pestaña, puede configurar el registro de eventos y las notificaciones de eventos. Los eventos se distribuyen según el nivel de importancia en las siguientes secciones:

- **Fallo operativo**
- **Advertencia**
- **Información**

Cada sección contiene una lista con los distintos tipos de eventos y la cantidad de días por los que cada evento se deja almacenado, de manera predeterminada, 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. Sin embargo, puede cambiar configuraciones específicas para los tipos de eventos requeridos.

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 mediante 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 activa la opción **Distribuir archivos solo mediante puntos de distribución**, asegúrese de que Kaspersky Security Center Linux esté configurado como origen de actualización en las tareas de actualización.

Esta opción está deshabilitada de manera predeterminada.

- [\*\*Tamaño máximo de la cola del evento, 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\*\*](#) 

El Agente de red instalado en un dispositivo administrado transfiere información sobre la directiva de aplicación de seguridad aplicada a la aplicación de seguridad (por ejemplo, Kaspersky Endpoint Security for Linux). 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 (o de la directiva fuera de la oficina) que se encontraba vigente cuando la directiva se entregó en el dispositivo administrado
- 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 directiva activos

Puede utilizar esta información para solucionar problemas o verificar que la directiva aplicada al dispositivo sea la esperada. Esta opción está deshabilitada de manera 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 manera 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 manera 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 habilitada de manera predeterminada.

- [Detalles de 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.

## Conectividad

La sección **Conectividad** incluye tres subsecciones:

- **Red**
- **Perfiles de conexión**
- **Programación de conexiones**

En la subsección **Red**, puede configurar la conexión con el Servidor de administración, activar el uso de un puerto UDP y especificar el número de puerto UDP.

- En el grupo de configuraciones **Conectar al 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 establezca el intervalo de sincronización (también conocido como heartbeat) 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 agrega un puerto UDP que el Agente de red necesita para funcionar a la lista de exclusiones del Firewall de Microsoft Windows.

Esta opción está habilitada de manera 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 habilitada de manera predeterminada.

- **Usar la puerta de enlace de conexión del 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 habilitada de manera predeterminada.

- **Usar puerto UDP** 

Si necesita que los dispositivos administrados se conecten al servidor proxy de KSN a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un número de **puerto UDP**. Esta opción está habilitada de manera predeterminada. El puerto UDP predeterminado de conexión al servidor proxy de KSN es 15111.

- [Número de puerto UDP](#) 

En este campo, puede indicar el número del puerto UDP. El número de puerto predeterminado es el 15000. El sistema decimal se usa para los registros.

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. Los ajustes de la sección **Perfiles de conexión** solo están disponibles en dispositivos que ejecutan Windows:

- [Configuración de la 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](#) 

Los perfiles de conexión solo son compatibles con dispositivos que ejecutan Windows.

Puede ver y añadir perfiles para la conexión del Agente de red al 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

- [Activar 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 manera 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 manera predeterminada.

- [Conectarse en los 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.

## Sondeo de la red realizado por los puntos de distribución

En la sección **Sondeo de la red realizado por los 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:

- [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 manera predeterminada.

- [Rangos IP](#) 

Si se activa esta opción, el punto de distribución sondeará automáticamente los rangos IP de acuerdo con la programación que ha configurado al hacer clic en el enlace **Programar sondeo**.

Si esta opción está desactivada, el punto de distribución no sondea rangos de 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 manera predeterminada.

- [Controladores de dominio](#) 

Si se activa esta opción, el punto de distribución sondeará automáticamente los controladores de dominio de acuerdo con la programación que ha configurado al hacer clic en el botón **Programar sondeo**.

Si esta opción está desactivada, el punto de distribución no sondea los controladores de dominio.

La frecuencia de sondeo del controlador 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 manera predeterminada.

## Configuración de red para puntos de distribución

En la sección **Configuración de red para puntos de distribución**, puede configurar los ajustes de acceso a Internet:

- Usar servidor proxy
- Dirección
- Número de puerto
- [No utilizar el servidor proxy para direcciones locales](#) <sup>?</sup>

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 manera predeterminada.

- [Autenticación del servidor proxy](#) <sup>?</sup>

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 configurar la aplicación para utilizar el punto de distribución para reenviar solicitudes de Kaspersky Security Network (KSN) desde los dispositivos administrados:

- [Activar el proxy de KSN en el punto de distribución](#) <sup>?</sup>

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.

Esta opción está deshabilitada de manera predeterminada. Esta opción solo se activa si las opciones **Utilizar el Servidor de administración como servidor proxy** y **Acepto usar Kaspersky Security Network** están activadas 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 de KSN al Servidor de administración](#) <sup>?</sup>

El punto de distribución envía las solicitudes KSN desde los dispositivos administrados al Servidor de administración.

Esta opción está habilitada de manera predeterminada.

- [Acceder a la nube de KSN/KPSN directamente a través de Internet](#) <sup>?</sup>



El punto de distribución envía las solicitudes KSN desde los dispositivos administrados a KSN Cloud o 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.

- **[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 el 13111.

- **[Puerto UDP](#)**

Si necesita que los dispositivos administrados se conecten al servidor proxy de KSN a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un número de **puerto UDP**. Esta opción está habilitada de manera predeterminada. El puerto UDP predeterminado de conexión al servidor proxy de KSN es 15111.

## 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 reinicios

En la sección **Administración de reinicios**, puede determinar la acción que 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. Los ajustes en **Administración de reinicios** están disponibles solo en dispositivos que ejecutan Windows:

- **[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 utilizando, 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 necesitan operar continuamente.

- **[Reiniciar el sistema operativo automáticamente de ser 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 manera 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 habilitada de manera predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles están entre 1 y 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 habilitada de manera predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- [Forzar el cierre de las 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 manera predeterminada.

## Uso del Agente de red para Windows, Linux y macOS: comparación

El uso del Agente de red varía según el sistema operativo del dispositivo. La directiva del Agente de red y la configuración del [paquete de instalación](#) 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, Linux y macOS.

Comparación de funciones del Agente de red

| Función del Agente de red | Windows | Linux | macOS |
|---------------------------|---------|-------|-------|
| <b>Instalación</b>        |         |       |       |

|                                                                                                                                                                                                                                                         |                                                                           |                                                                                                                                                               |                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| <a href="#">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</a> | ✓                                                                         | ✓                                                                                                                                                             | —                                                              |
| Instalación con herramientas de terceros para la instalación remota de aplicaciones                                                                                                                                                                     | ✓                                                                         | ✓                                                                                                                                                             | ✓                                                              |
| Instalación manual, ejecutando el instalador de la aplicación en los dispositivos                                                                                                                                                                       | ✓                                                                         | ✓                                                                                                                                                             | ✓                                                              |
| <a href="#">Instalación del Agente de red en modo silencioso</a>                                                                                                                                                                                        | ✓                                                                         | ✓                                                                                                                                                             | ✓                                                              |
| 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                                                                                                                                                                                                                                  | ✓                                                                         | ✓                                                                                                                                                             | ✓                                                              |
| <b>Punto de distribución</b>                                                                                                                                                                                                                            |                                                                           |                                                                                                                                                               |                                                                |
| <a href="#">Uso como punto de distribución</a>                                                                                                                                                                                                          | ✓                                                                         | ✓                                                                                                                                                             | ✓                                                              |
| <a href="#">Designación automática de puntos de distribución</a>                                                                                                                                                                                        | ✓                                                                         | ✓<br>Sin utilizar el reconocimiento de ubicación de red (NLA).                                                                                                | ✓<br>Sin utilizar el reconocimiento de ubicación de red (NLA). |
| Modelo de descarga de actualizaciones sin conexión                                                                                                                                                                                                      | ✓                                                                         | ✓                                                                                                                                                             | ✓                                                              |
| Sondeo de red                                                                                                                                                                                                                                           | ✓<br>• Sondeo de intervalos IP<br><br>• Sondeo del controlador de dominio | ✓<br>• Sondeo de intervalos IP<br><br>• Sondeo con Zeroconf<br><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 actualizaciones de Kaspersky a los repositorios de los puntos de distribución que se utilizan para distribuir 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). |
| 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                                                                                                                                                                                                   | ✓ | ✓                                                                                                                                   | —                                                                                                                                                                                                                                                                              |
| <b>Administración de aplicaciones de terceros</b>                                                                                                                                                                        |   |                                                                                                                                     |                                                                                                                                                                                                                                                                                |
| <a href="#">Instalación remota de aplicaciones en dispositivos</a>                                                                                                                                                       | ✓ | —                                                                                                                                   | —                                                                                                                                                                                                                                                                              |
| 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                                                                                                                                                                    | ✓ | —                                                                                                                                   | —                                                                                                                                                                                                                                                                              |
| Instalación de actualizaciones de software                                                                                                                                                                               | ✓ | —                                                                                                                                   | —                                                                                                                                                                                                                                                                              |
| Inventariado del software instalado en los dispositivos                                                                                                                                                                  | ✓ | ✓                                                                                                                                   | —                                                                                                                                                                                                                                                                              |
| <b>Máquinas virtuales</b>                                                                                                                                                                                                |   |                                                                                                                                     |                                                                                                                                                                                                                                                                                |
| <a href="#">Instalación del Agente de red en una máquina virtual</a>                                                                                                                                                     | ✓ | ✓                                                                                                                                   | ✓                                                                                                                                                                                                                                                                              |
| <a href="#">Optimización de la configuración para infraestructuras de escritorios virtuales (VDI)</a>                                                                                                                    | ✓ | ✓                                                                                                                                   | ✓                                                                                                                                                                                                                                                                              |
| <a href="#">Compatibilidad con máquinas virtuales dinámicas</a>                                                                                                                                                          | ✓ | ✓                                                                                                                                   | ✓                                                                                                                                                                                                                                                                              |
| <b>Otro</b>                                                                                                                                                                                                              |   |                                                                                                                                     |                                                                                                                                                                                                                                                                                |
| Acciones de auditoría en dispositivos cliente remotos                                                                                                                                                                    | ✓ | —                                                                                                                                   | —                                                                                                                                                                                                                                                                              |

|                                                                                                                               |   |   |                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------|---|---|---------------------------------------------------------------------------------------------------|
| mediante Windows Desktop Sharing                                                                                              |   |   |                                                                                                   |
| Supervisión del estado de protección antivirus                                                                                | ✓ | ✓ | ✓                                                                                                 |
| Administración del reinicio de los dispositivos                                                                               | ✓ | — | —                                                                                                 |
| <a href="#">Compatibilidad con las reversiones de estado en los sistemas de archivos</a>                                      | ✓ | ✓ | ✓                                                                                                 |
| 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 (en 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) |
| Descarga de un paquete de instalación independiente a través del Asistente de migración                                       | ✓ | ✓ | ✓                                                                                                 |

## Comparación de la configuración del Agente de red por sistemas operativos

La siguiente tabla muestra qué configuraciones del Agente de red están disponibles según el sistema operativo del dispositivo administrado en el que se instaló el Agente de red.

Configuración del Agente de red: comparación por sistemas operativos

| Sección Configuración    | Windows | Linux                                                                                                                                                                                                                                                                                              | macOS |
|--------------------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| General                  | ✓       | ✓                                                                                                                                                                                                                                                                                                  | ✓     |
| Configuración de eventos | ✓       | ✓                                                                                                                                                                                                                                                                                                  | ✓     |
| Configuración            | ✓       | ✓<br>Las siguientes opciones están disponibles: <ul style="list-style-type: none"> <li>• Distribuir archivos solo mediante puntos de distribución</li> <li>• Tamaño máximo de la cola del evento, en MB</li> <li>• La aplicación podrá obtener información adicional sobre la directiva</li> </ul> | ✓     |

|                                                           |                                                                                                                                                                                                             | en el dispositivo                                                                                                                                                                                                |   |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| Repositorios                                              | ✓                                                                                                                                                                                                           | <p>✓</p> <p>Las siguientes opciones están disponibles:</p> <ul style="list-style-type: none"> <li>• <b>Detalles de las aplicaciones instaladas</b></li> <li>• <b>Detalles de registro de hardware</b></li> </ul> | — |
| Conectividad → Red                                        | ✓                                                                                                                                                                                                           | <p>✓</p> <p>Excepto la opción <b>Abrir puertos del Agente de red en el Firewall de Microsoft Windows</b>.</p>                                                                                                    | ✓ |
| Conectividad → Perfiles de conexión                       | ✓                                                                                                                                                                                                           | —                                                                                                                                                                                                                | ✓ |
| Conectividad → Programación de conexiones                 | ✓                                                                                                                                                                                                           | ✓                                                                                                                                                                                                                | ✓ |
| Sondeo de la red realizado por los puntos de distribución | <p>✓</p> <p>Las siguientes opciones están disponibles:</p> <ul style="list-style-type: none"> <li>• <b>Red de Windows</b></li> <li>• <b>Rangos IP</b></li> <li>• <b>Controladores de dominio</b></li> </ul> | <p>✓</p> <p>Las siguientes opciones están disponibles:</p> <ul style="list-style-type: none"> <li>• <b>Zeroconf</b></li> <li>• <b>Rangos IP</b></li> <li>• <b>Controladores de dominio</b></li> </ul>            | — |
| Configuración de red para puntos de distribución          | ✓                                                                                                                                                                                                           | ✓                                                                                                                                                                                                                | ✓ |
| Proxy de KSN (puntos de distribución)                     | ✓                                                                                                                                                                                                           | ✓                                                                                                                                                                                                                | — |
| Actualizaciones (puntos de distribución)                  | ✓                                                                                                                                                                                                           | ✓                                                                                                                                                                                                                | — |
| Historial de revisión                                     | ✓                                                                                                                                                                                                           | ✓                                                                                                                                                                                                                | ✓ |

## 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 **Utilizar proxy de KSN** esté habilitada. Esta función ayuda a redistribuir y optimizar el tráfico de la red.

Si utiliza [Managed Detection and Response](#), debe activar la opción [Proxy de KSN](#) para el punto de distribución y [activar el modo de KSN extendido](#).

5. [opcional] Active el uso de servidores KSN si el servicio de proxy de KSN no está disponible. Los servidores de KSN pueden estar localizados en el lado de Kaspersky (cuando se usa KSN) o en el lado de terceros (cuando se usa 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 antivirus, 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 para 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.

## Desactivación del análisis de los dispositivos de red

Cuando Kaspersky Endpoint Security para Windows analiza las unidades de red, estas pueden sufrir una carga importante. Resulta más cómodo realizar un análisis indirecto en los servidores de archivo.

Puede desactivar el análisis de las 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 de amenaza esencial** → **Protección frente a amenazas en archivos**.
4. En **Cobertura de la protección**, desactive la opción **Todas las unidades de red**.
5. Haga clic en **Aceptar**.

El análisis de unidades de red está desactivado.

## 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 almacenamiento**.
4. En **Transferencia de datos al Servidor de administración**, si aún está habilitada en la directiva de nivel superior, deshabilite la casilla de verificación **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 el disco en la base de datos de Kaspersky Security Center Linux (docenas de gigabytes).

La base de datos del Servidor de administración ya no contendrá información sobre los módulos de software instalados.

## Configuración del acceso a la interfaz de Kaspersky Endpoint Security para Windows en estaciones de trabajo

Si la protección antivirus en la red de la organización se debe administrar en modo centralizado a través de Kaspersky Security Center Linux, especifique la configuración de la interfaz en las propiedades de la directiva de Kaspersky Endpoint Security para Windows, como se describe a continuación. Como resultado, evitará el acceso no autorizado a Kaspersky Endpoint Security para Windows en las estaciones de trabajo y el cambio de la configuración 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 especificar la configuración de interfaz recomendada:*

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 **Sin interfaz**. Esto desactiva la visualización de la interfaz de usuario de Kaspersky Endpoint Security para Windows en las estaciones de trabajo, por lo que sus usuarios no pueden cambiar la configuración de Kaspersky Endpoint Security para Windows.
5. En **Protección de contraseña**, habilite el interruptor de palanca. Esto reduce el riesgo de cambios no autorizados o no deseados en la configuración de Kaspersky Endpoint Security para Windows en estaciones de trabajo.

Se especifican las configuraciones recomendadas 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 **Añadir evento** y active únicamente las casillas de verificación ubicadas junto a los siguientes eventos:
  - *Contrato de licencia de usuario final infringido*
  - *La ejecución automática de la aplicación está deshabilitada*
  - *Error de activación*
  - *Se detectó una amenaza activa; Se debe iniciar la Desinfección avanzada*
  - *Desinfección imposible*
  - *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 en 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 **Fallo operativo**, haga clic en **Añadir 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 **Añadir evento** y seleccione las casillas de verificación solo junto a los siguientes eventos:

- *La Autoprotección está deshabilitada*
- *Componentes de protección deshabilitados*
- *Clave de reserva incorrecta*
- *Se detectó software con fines lícitos que intrusos podrían usar para dañar el equipo o sus datos personales (bases de datos locales)*
- *Se detectó software con fines lícitos que intrusos podrían usar para dañar el 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 en el servidor de Kaspersky Anti Targeted Attack Platform*
- *El administrador puso el archivo en cuarentena en el servidor Kaspersky Anti Targeted Attack Platform*
- *Mensaje para el administrador sobre la prohibición de inicio de la aplicación*
- *Mensaje al administrador sobre la prohibición de acceso al dispositivo*
- *Mensaje al administrador sobre la prohibición de acceso a la página web*

9. Haga clic en **Aceptar**.

10. En la sección **Información**, haga clic en **Añadir evento** y seleccione las casillas de verificación 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 **Cuando se descargan nuevas actualizaciones en el repositorio** cuando la casilla de verificación **Usar el retraso aleatorio automáticamente para el inicio de tareas** está seleccionada.

## 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.

## 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.

Al participar en el programa KSN, acepta enviar automáticamente a Kaspersky información sobre el funcionamiento de las aplicaciones Kaspersky instaladas en los dispositivos cliente administrados por Kaspersky Security Center Linux. La información se transfiere de conformidad con la [configuración de acceso a KSN](#).

Kaspersky Security Center Linux es compatible con las siguientes soluciones de infraestructura de KSN:

- *KSN Global*. Esta solución permite intercambiar información con Kaspersky Security Network. Si participa en el programa KSN, acepta enviar automáticamente a Kaspersky información sobre el funcionamiento de las aplicaciones Kaspersky instaladas en los dispositivos cliente administrados por Kaspersky Security Center Linux. 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 Linux 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 desde sus propios equipos. KPSN está 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 solicita que se una a KSN durante la ejecución del [asistente de inicio rápido](#). Puede comenzar a utilizar KSN o dejar de hacerlo en cualquier momento que se encuentre [utilizando 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 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 anterior de la Declaración de KSN que aceptó anteriormente.

Cuando KSN está activado, Kaspersky Security Center Linux comprueba si se puede acceder a los servidores de KSN. Si no es posible acceder a los servidores mediante el DNS del sistema, la aplicación utiliza [servidores de 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 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.

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 **Activar proxy de KSN en el Servidor de administración Activada**.

Los datos se envían desde los dispositivos cliente a KSN de acuerdo con la directiva de Kaspersky Endpoint Security activa en esos dispositivos. Si esta casilla está vacía, no se enviará ningún dato a KSN desde el Servidor de administración y los dispositivos cliente mediante Kaspersky Security Center Linux. Sin embargo, los dispositivos cliente pueden enviar datos directamente a KSN (omitiendo Kaspersky Security Center Linux), de conformidad con sus respectivas configuraciones. La directiva de Kaspersky Endpoint Security, que está activa en los dispositivos cliente determina qué datos enviarán directamente (omitiendo Kaspersky Security Center Linux) dichos dispositivos a KSN.

4. Cambie el interruptor a la posición **Usar Kaspersky Security Network Activada**.

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 de activación a la posición **Usar Kaspersky Private Security Network Activada** y haga clic en el botón **Seleccionar archivo con la configuración del proxy de KSN** para descargar la configuración de KPSN (archivos con las extensiones pkcs7 y pem). Después de descargar la configuración, la interfaz muestra el nombre y los contactos del proveedor, así como la fecha de creación del archivo con la configuración de KPSN.

Cuando cambie el botón de activación a la posición **Usar Kaspersky Private Security Network Activada**, aparecerá un mensaje con los detalles sobre KPSN.

Las siguientes aplicaciones de Kaspersky son compatibles con KPSN:

- Kaspersky Security Center Linux
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security para Windows

Si activa KPSN en Kaspersky Security Center Linux, estas aplicaciones reciben información sobre la compatibilidad con KPSN. En la ventana de configuración de la aplicación, en la subsección **Kaspersky Security Network** de la sección **Protección avanzada contra amenazas**, se muestra la información sobre el proveedor de KSN: KSN o KPSN.

Kaspersky Security Center Linux no envía ningún dato estadístico a Kaspersky Security Network si KPSN está configurada 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, active la opción **Ignorar la configuración del servidor proxy al 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.

7. Cambie el botón de alternancia a la posición **Conectar Servidores de administración secundarios a KSN mediante el Servidor de administración principal Activada**.

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 **Activar proxy de KSN en el Servidor de administración Activada**.

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 **Activar el proxy de KSN en el punto de distribución** y, a continuación, habilite la opción **Acceder a la nube de KSN/KPSN directamente a través de Internet**.
6. Haga clic en **Aceptar**.

El punto de distribución actuará como servidor proxy de KSN.

Tenga en cuenta que el punto de distribución no admite la autenticación de dispositivos administrados mediante el protocolo NTLM.

## Habilitar y deshabilitar KSN

*Para habilitar 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 **Activar proxy de KSN en el Servidor de administración Activada**.  
Se habilita el servidor proxy de KSN.
4. Cambie el interruptor a la posición **Usar Kaspersky Security Network Activada**.  
KSN se habilitará.  
Si se habilita el botón de activación, los dispositivos cliente enviarán los resultados de instalación de parches a Kaspersky. Al seleccionar este botón de activación, debe leer y aceptar los términos de la Declaración de KSN.
5. Haga clic en el botón **Guardar**.

*Para deshabilitar 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. Ponga el interruptor en la posición **Activar proxy de KSN en el Servidor de administración Desactivada** para deshabilitar el servicio del proxy de KSN, o ponga el interruptor en la posición **Usar Kaspersky Security Network Desactivada**.

Si alguno de estos interruptores está deshabilitado, los dispositivos cliente no enviarán los resultados de instalación del parche a Kaspersky.

Si utiliza KPSN, cambie el botón de activación a la posición **Usar Kaspersky Private Security Network Desactivada**.

KSN se deshabilitará.

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 muestra cuando actualiza el 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 o mejorar el 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

En un dispositivo administrado asignado para funcionar como punto de distribución, puede habilitar el Kaspersky Security Network (KSN) Proxy. Un dispositivo administrado funciona como el servidor proxy de KSN cuando el servicio ksnproxy se está ejecutando en el dispositivo. 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 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. Revise la lista de procesos en ejecución para verificar si se está ejecutando el proceso `/opt/kaspersky/ksc64/sbin/ksnproxy`.

Que el servicio `/opt/kaspersky/ksc64/sbin/ksnproxy` esté en ejecución indica que el Agente de red del dispositivo participa en Kaspersky Security Network y funciona como proxy de KSN para los dispositivos administrados incluidos en el alcance del 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.

## Administración de tareas

Esta sección describe tareas utilizadas por Kaspersky Security Center Linux.

## Acerca de las tareas

Kaspersky Security Center Linux administra las aplicaciones de seguridad de Kaspersky instaladas en 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 Kaspersky Security Center Web Console, o por el usuario de un dispositivo remoto (por ejemplo, a través de la interfaz de la aplicación 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*: tareas que se realizan en un conjunto de dispositivos, independientemente de si están incluidos en algún 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.  
Puede utilizar una dirección IP (o un rango IP) o un nombre DNS como la dirección del dispositivo.
- Importación de una lista de dispositivos desde un archivo .txt con las direcciones del dispositivo que se añadirán (cada dirección debe ubicarse en una línea individual).

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 **Añadir**.  
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 tareas**. 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 tarea** y, luego, seleccione **Añadir 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 manualmente en cualquier momento desde la lista de tareas; o seleccione dispositivos en la lista **Dispositivos administrados** y, luego, inicie 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, active la casilla de verificación 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 Linux.

*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 *Instalar aplicación en remoto* está relacionada con el Servidor de administración, mientras que la tarea *Actualizar* corresponde a Kaspersky Endpoint Security.

*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 utilizando, 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 necesitan 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.

- [Forzar el cierre de las 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 manera predeterminada.

- Programación de 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 forma predeterminada, la tarea se ejecutará cada seis 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. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center Linux.

De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

- **Semanalmente** 

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 p. m.

- **Mensualmente** 

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.

- **Manualmente** 

La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

Esta opción está habilitada de manera predeterminada.

- **Cada mes, en días concretos de las semanas seleccionadas** 

La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es a las 6:00:00 p. m.

- **Cuando se descargan nuevas actualizaciones en el repositorio** 

La tarea se ejecuta después de descargar las actualizaciones en el repositorio. Por ejemplo, es posible que desee utilizar esta programación para la tarea *Actualizar*.

- **Al completar otra tarea** 

La tarea actual se iniciará después de que se complete otra tarea. Puede seleccionar cómo se deberá completar esa tarea anterior (correctamente o con errores) para que se dé inicio a la tarea subsiguiente. Este parámetro solo funciona si ambas tareas están asignadas a los mismos dispositivos.

- **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 **Manualmente, 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 se ejecutarán las tareas programadas en los dispositivos cliente; las tareas con las opciones de programación **Manualmente, Una vez** e **Inmediatamente** solo se ejecutarán en aquellos dispositivos cliente que estén 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 habilitada de manera predeterminada.

- [Usar el retraso aleatorio automáticamente 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.

- [Usar el retraso aleatorio para el inicio de tareas con un intervalo de \(min\)](#) 

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 manera 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 DNS, direcciones IP y subredes IP de dispositivos a los cuales debe asignar la tarea.

Puede 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 en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred 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 resultarle útil para, por ejemplo, ejecutar una tarea en 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.

- 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 manera 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 activada, la [cobertura de la tarea](#) incluye:

- El grupo de administración que se seleccionó al crear la tarea.
- Los grupos de administración subordinados al grupo de administración seleccionado en cualquier nivel inferior al de la [jerarquía del grupo](#).

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 habilitada de manera 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 manera 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 los dispositivos después de completar la tarea**. Encontrará esta opción en la misma ventana.

Esta opción está deshabilitada de manera 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 manera 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 manera predeterminada. El tiempo de ejecución por defecto para las tareas es de 120 minutos.

- Ajustes de notificaciones:

- Bloque **Almacenar el historial de la tarea:**

- [Almacenar en la base de datos del Servidor de administración durante \(días\)](#) ⓘ

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 habilitada de manera predeterminada.

- [Almacenar en el registro de eventos del SO del dispositivo](#) ⓘ

Los eventos de la aplicación relacionados con la ejecución de la tarea se almacenan localmente en el Registro de eventos de Syslog de cada dispositivo cliente.

Esta opción está deshabilitada de manera predeterminada.

- [Almacenar en el registro de eventos del SO del Servidor de administración](#) ⓘ

Los eventos de la aplicación relacionados con la ejecución de la tarea en todos los dispositivos cliente del ámbito de la tarea se almacenan de forma centralizada en el Registro de eventos de Syslog del sistema operativo (SO) del Servidor de administración.

Esta opción está deshabilitada de manera 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 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 de 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 habilitada de manera 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 de la cobertura 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 Linux le permite guardar una tarea y su configuración en un archivo KLT. Puede utilizar este archivo KLT para [importar la tarea guardada](#) a Kaspersky Security Center Windows y a Kaspersky Security Center Linux.

*Para exportar una tarea:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.

2. Marque la casilla que hay junto a la tarea que desea exportar.

No puede exportar varias tareas al mismo tiempo. Si selecciona más de una tarea, el botón **Exportar** se desactivará. Las tareas del Servidor de administración tampoco están disponibles para exportarse.

3. Haga clic en el botón **Exportar**.

4. En la ventana **Guardar como** abierta, especifique la ruta y el nombre del archivo de la tarea. Haga clic en el botón **Guardar**.

La ventana **Guardar como** se muestra solo si usa Google Chrome, Microsoft Edge u Opera. Si utiliza otro navegador, el archivo de la tarea se guarda automáticamente en la carpeta **Descargas**.

## Importar una tarea

Kaspersky Security Center Linux le permite importar una tarea desde 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 abierta, especifique la ruta al archivo de la tarea KLT y haga clic en el botón **Abrir**. Tenga en cuenta que solo puede seleccionar un archivo de tarea.

Comienza el procesamiento de la tarea.

5. Después de que la tarea se procese correctamente, seleccione los dispositivos a los que desea asignarla. Para hacerlo, 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.

- [Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista](#) ⓘ

Puede especificar nombres DNS, direcciones IP y subredes IP de dispositivos a los cuales debe asignar la tarea.

Puede 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 en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred 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 resultarle útil para, por ejemplo, ejecutar una tarea en dispositivos que tengan una versión específica de un sistema operativo.

6. Especifique la cobertura de la tarea.

7. Haga clic en el botón **Completar** para finalizar la importación de la tarea.

Aparece la 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.

Después de una importación correcta, la tarea aparece en la lista de tareas. La configuración y la programación de la tarea también se importan. 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)**.

## Inicio del 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 le permite reemplazar automáticamente la contraseña anterior por la nueva en todas las tareas en las que se especifica la cuenta. 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 que sean válidas en su sistema. Cuando cambia al siguiente paso del asistente, Kaspersky Security Center Linux 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 utiliza el nombre de la cuenta con la que ha iniciado sesión actualmente en Kaspersky Security Center Web Console. Usted deberá escribir la contraseña de dicha cuenta en el campo **Contraseña actual para utilizar en 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 tareas**.

Si completa el campo **Contraseña anterior (opcional; si desea sustituirla por la actual)**, Kaspersky Security Center Linux 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 elegidas se aplican después de pasar al siguiente paso del asistente.

## Paso 3. Ver los resultados

En el último paso del asistente, vea los resultados de cada una de las tareas encontradas. Para completar el Asistente, haga clic en el botón **Finalizar**.

## Ver resultados de la ejecución de tareas almacenados en el Servidor de administración

Kaspersky Security Center Linux le permite ver los resultados de las tareas de grupo, las tareas asignadas a dispositivos específicos y las tareas del Servidor de administración. No se pueden ver resultados de la ejecución para tareas locales.

*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**.

## Etiquetas de aplicación

En esta sección, se explica qué son las etiquetas para aplicaciones y se ofrecen instrucciones para crearlas y modificarlas, así como para etiquetar aplicaciones de terceros.

## Acerca de las etiquetas de aplicación

Kaspersky Security Center Linux le permite etiquetar aplicaciones de terceros (aplicaciones creadas por vendedores de software diferentes a Kaspersky). 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 la aplicación**.
2. Haga clic en **Añadir**.  
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 la aplicación**.



2. Active la casilla de verificación 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 de verificación activada en la columna **Etiqueta asignada**.

4. Busque las etiquetas que desee asignar y active las casillas de verificación correspondientes en la columna **Etiqueta asignada**.

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 de verificación activada en la columna **Etiqueta asignada**.

4. Busque las etiquetas que desee quitarle a la aplicación y desactive las casillas de verificación correspondientes en la columna **Etiqueta asignada**.

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 la 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.

## 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 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 que ha bloqueado Control de dispositivos si la opción **Permitir solicitud de acceso temporal** está activada en la configuración de la directiva de Kaspersky Endpoint Security, en la sección **Configuración de la aplicación** → **Controles de seguridad** → **Control del dispositivo** sección.

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, 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 Linux.
2. Al recibir esta solicitud, el administrador de Kaspersky Security Center Linux crea un archivo clave de acceso y lo envía al usuario del dispositivo.
3. En la ventana de diálogo de Kaspersky Endpoint Security, el usuario del dispositivo activa el archivo clave de acceso y puede acceder de manera 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 **Conceder acceso al dispositivo en modo desconectado**.
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 valor de la configuración del **Período de activación**.  
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**.
9. En la ventana que se abre, 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**.

En conclusión, cuando envía al usuario el archivo con la clave de acceso para que lo active en la ventana de diálogo de Kaspersky Endpoint Security, el usuario tiene acceso temporal al dispositivo bloqueado durante el período especificado.

## Uso de la utilidad klscflag para abrir el puerto 13291

El Servidor de administración utiliza el puerto 13291 para recibir conexiones de la Consola de administración basada en MMC. En ordenadores que no usan Windows, este puerto está cerrado de forma predeterminada.

Si desea permitir la conexión a la Consola de administración basada en MMC o la utilidad klakaut, puede abrir este puerto mediante la utilidad klscflag. Tenga en cuenta que la funcionalidad de la Consola de administración basada en MMC se reduce cuando se conecta a Kaspersky Security Center Linux. Le recomendamos que utilice Kaspersky Security Center Web Console para conectarse a Kaspersky Security Center Linux.

La utilidad cambia el valor del parámetro KLSRV\_SP\_SERVER\_SSL\_PORT\_GUI\_OPEN.

Le recomendamos que utilice Kaspersky Security Center Web Console para conectarse a Kaspersky Security Center Linux.

Para abrir el puerto 13291:

1. Ejecute el siguiente comando en la línea de comandos:

```
$ /opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type =
\"SS_SETTINGS\";"
```

2. Reinicie el servicio del Servidor de administración de Kaspersky Security Center con el siguiente comando:

```
$ sudo systemctl restart kladminserver_srv
```

El puerto 13291 queda abierto.

Para comprobar si el puerto 13291 se ha abierto correctamente:

Ejecute el siguiente comando en la línea de comandos:

```
$ /opt/kaspersky/ksc64/sbin/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>true
```

El valor `true` significa que el puerto está abierto. De lo contrario, se muestra el valor `false`.

## Registro de la aplicación Kaspersky Industrial CyberSecurity for Networks en Kaspersky Security Center Web Console

Para comenzar a trabajar con la aplicación Kaspersky Industrial CyberSecurity for Networks a través de Kaspersky Security Center Web Console, primero debe registrarla en Kaspersky Security Center Web Console.

Para registrar la aplicación Kaspersky Industrial CyberSecurity for Networks, siga estos pasos:

1. Asegúrese de que se cumplan estos requisitos:

- Ha [descargado e instalado el complemento web de Kaspersky Industrial CyberSecurity for Networks](#). Puede hacerlo más adelante mientras espera que el servidor de Kaspersky Industrial CyberSecurity for Networks se sincronice con el Servidor de administración. Después de descargar e instalar el complemento, se muestra la sección **KICS para redes** en el menú principal de Kaspersky Security Center Web Console.
- En la interfaz web de Kaspersky Industrial CyberSecurity for Networks, se configura y activa la interacción con Kaspersky Security Center. Para obtener más información, consulte la [Ayuda en línea de Kaspersky Industrial CyberSecurity for Networks](#).

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 ubicada junto al dispositivo donde está instalado el servidor de Kaspersky Industrial CyberSecurity for Networks.
  - c. Haga clic en el botón **Mover a un grupo**.
  - d. En la jerarquía de grupos de administración, seleccione la casilla ubicada junto al grupo **Dispositivos administrados**.
  - e. Haga clic en el botón **Mover**.
3. Abra la ventana de propiedades del dispositivo donde está instalado el servidor de Kaspersky Industrial CyberSecurity for Networks.
  4. En la página de propiedades del dispositivo, en la sección **General**, seleccione la opción **No desconectar 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 Security Center.
  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.
  8. ☺ Si desea ver las estadísticas de Kaspersky Industrial CyberSecurity for Networks, puede añadir widgets en el panel. Para añadir los widgets, haga lo siguiente:
    - a. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
    - b. En el panel, haga clic en el botón **Añadir o restaurar un widget web**.
    - c. En el menú del widget que se abre, seleccione **Otros**.
    - d. Seleccione los widgets que desee añadir:
      - Mapa de despliegue de KICS para redes
      - Información sobre los servidores KICS para redes
      - Eventos actualizados de KICS para redes
      - Dispositivos con problemas en KICS para redes
      - Eventos críticos en KICS para redes
      - Estados en KICS para redes
9. Para acceder a la interfaz web de Kaspersky Industrial CyberSecurity for Networks, haga lo siguiente:
    - a. En el menú principal, vaya a **KICS para redes** → **Buscar**.
    - b. Haga clic en el botón **Buscar eventos o dispositivos**.
    - c. En la ventana **Parámetros de consulta** que se abre, haga clic en el campo **Servidor**.

- d. Seleccione el servidor de Kaspersky Industrial CyberSecurity for Networks de la lista desplegable de servidores integrados con Kaspersky Security Center y, a continuación, haga clic en el botón **Buscar**.
- e. Haga clic en el enlace **Ir al servidor** ubicado junto al nombre del servidor de Kaspersky Industrial CyberSecurity for Networks.

Se muestra la página de inicio de sesión de Kaspersky Industrial CyberSecurity for Networks.

Para iniciar sesión en la interfaz web de Kaspersky Industrial CyberSecurity for Networks, debe proporcionar las credenciales de la cuenta de usuario de la aplicación.

# Administración de 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 las cuentas de usuario

Kaspersky Security Center Linux le permite administrar cuentas de usuario y grupos de seguridad. La aplicación admite dos tipos de cuentas:

- Cuentas de empleados de la organización. El Servidor de administración recupera los datos de las cuentas de esos usuarios locales cuando sondea la red de la organización.
- Cuentas de usuarios internos de Kaspersky Security Center Linux. Puede crear cuentas de usuarios internos en el portal. Estas cuentas se utilizan solo en Kaspersky Security Center Linux.

*Para ver las tablas de cuentas de usuario y los grupos de seguridad, haga lo siguiente:*

1. En el menú principal, vaya a **Usuarios y funciones** → **Usuarios y grupos**.
2. Seleccione la pestaña **Usuarios** o **Grupos**.

Se abre la tabla de usuarios o grupos de seguridad. Si desea ver la tabla solo con usuarios o grupos internos o solo con usuarios o grupos locales, configure los criterios de filtro **Subtipo** en **Interno** o **Local**, respectivamente.

## 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 una función 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 gestiona 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.

## Configurar los derechos de acceso a las funciones de la aplicación. Control de acceso basado en roles

Kaspersky Security Center Linux proporciona recursos para el acceso basado en funciones a las funciones de Kaspersky Security Center Linux o las aplicaciones administradas de Kaspersky.

Puede configurar [los derechos de acceso a las funciones de la aplicación](#) para los usuarios de Kaspersky Security Center Linux 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

La siguiente tabla muestra las funciones de Kaspersky Security Center Linux con los derechos de acceso para administrar las tareas, informes y configuraciones asociados y realizar las acciones de 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 de **lectura**, **escritura** y **ejecución** pueden aplicarse a cualquier tarea, informe o configuración. Además de estos tres derechos, para administrar tareas, informes o ajustes en selecciones de dispositivos, el usuario debe tener el derecho **Realizar operaciones en selecciones de dispositivos**.



Todas las tareas, informes, ajustes de configuración y paquetes de instalación que no figuran en la tabla pertenecen al área funcional **Características generales: Funcionalidad básica**.

Derechos de acceso a las funciones de la aplicación

| Área funcional                                                                   | Derecho                                                                                                                                                                                      | Acción del usuario:<br>derecho necesario para<br>realizar la acción                                                                                                                                                                                                                                                                                                                                     | Tarea                                                                                                                                                                                                                                                                                                       | Informe                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Características generales:<br/>Administración de grupos de administración</b> | <b>Escritura</b>                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• Añadir dispositivos a un grupo de administración: <b>Escritura</b></li> <li>• Eliminar dispositivos de un grupo de administración: <b>Escritura</b></li> <li>• Agregar un grupo de administración a otro grupo de administración: <b>Escritura</b></li> <li>• Eliminar un grupo de administración de otro grupo de administración: <b>Escritura</b></li> </ul> | Ninguno                                                                                                                                                                                                                                                                                                     | N/C                                                                                                                                                                                                                                                                                     |
| <b>Características generales:<br/>Acceder a objetos sin importar sus ACL</b>     | <b>Leer</b>                                                                                                                                                                                  | Obtener acceso de lectura a todos los objetos: <b>Leer</b>                                                                                                                                                                                                                                                                                                                                              | Ninguno                                                                                                                                                                                                                                                                                                     | N/C                                                                                                                                                                                                                                                                                     |
| <b>Características generales:<br/>Funcionalidad básica</b>                       | <ul style="list-style-type: none"> <li>• <b>Leer</b></li> <li>• <b>Escritura</b></li> <li>• <b>Ejecutar</b></li> <li>• <b>Realizar operaciones en selecciones de dispositivos</b></li> </ul> | <ul style="list-style-type: none"> <li>• Reglas de movimiento de dispositivos (crear, modificar o eliminar) para el Servidor virtual: <b>Escritura, realizar operaciones en selecciones de dispositivos</b></li> <li>• Obtener certificado personalizado del protocolo móvil (LWNGT): <b>Lectura</b></li> <li>• Establecer certificado personalizado del</li> </ul>                                     | <ul style="list-style-type: none"> <li>• "Descargar actualizaciones en el repositorio del Servidor de administración"</li> <li>• "Entregar informes"</li> <li>• "Distribuir paquete de instalación"</li> <li>• "Instalar aplicación en Servidores de administración secundarios de forma remota"</li> </ul> | <ul style="list-style-type: none"> <li>• "Informe del estado de la protección"</li> <li>• "Informe de amenazas"</li> <li>• "Informe de los dispositivos más infectados"</li> <li>• "Informe sobre el estado de las bases de datos antivirus"</li> <li>• "Informe de errores"</li> </ul> |

protocolo móvil (LWNGT): **Escribir**

- Obtener la lista de redes definidas por NLA: **Leer**
- Añadir, modificar o eliminar una lista de redes definida por NLA: **Escritura**
- Ver la lista de control de acceso de los grupos: **Leer**
- Ver el registro del sistema operativo: **Leer**

- "Informe de ataques de red"
- "Informe conciso sobre las aplicaciones instaladas para la defensa del perímetro"
- "Informe conciso sobre los tipos de aplicaciones instaladas"
- "Informe sobre usuarios de dispositivos infectados"
- "Informe sobre problemas de seguridad"
- "Informe de eventos"
- "Informe de actividad de puntos de distribución"
- "Informe sobre Servidores de administración"
- "Informe sobre los eventos de Control de dispositivos"
- "Informe sobre aplicaciones prohibidas"
- "Informe de Control web"
- "Informe sobre el estado del cifrado de los dispositivos administrados"
- "Informe sobre el estado del cifrado de los

|                                                                              |                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                           |         |                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                              |                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                           |         | <p>dispositivos de almacenamiento masivo"</p> <ul style="list-style-type: none"> <li>• "Informe sobre los derechos de acceso a dispositivos cifrados"</li> <li>• "Informe sobre errores en el cifrado de archivos"</li> <li>• "Informe sobre el bloqueo del acceso a archivos cifrados"</li> <li>• "Informe sobre permisos de usuario vigentes"</li> <li>• "Informe sobre derechos"</li> </ul> |
| <p><b>Características generales:</b><br/><b>Objetos eliminados</b></p>       | <ul style="list-style-type: none"> <li>• Leer</li> <li>• Escritura</li> </ul>                                                                                                                                               | <ul style="list-style-type: none"> <li>• Ver objetos eliminados en la Papelera de reciclaje: <b>Leer</b></li> <li>• Eliminar objetos de la Papelera de reciclaje: <b>Escritura</b></li> </ul>                                                                                                                                             | Ninguno | N/C                                                                                                                                                                                                                                                                                                                                                                                            |
| <p><b>Características generales:</b><br/><b>Procesamiento de eventos</b></p> | <ul style="list-style-type: none"> <li>• Eliminar eventos</li> <li>• Editar la configuración de notificaciones sobre los eventos</li> <li>• Editar la configuración del registro de eventos</li> <li>• Escritura</li> </ul> | <ul style="list-style-type: none"> <li>• Cambiar los ajustes de registro de eventos: <b>Editar la configuración de registro de eventos</b></li> <li>• Cambiar los ajustes de las notificaciones sobre los eventos: <b>Editar configuración de notificación de eventos</b></li> <li>• Eliminar eventos: <b>Eliminar eventos</b></li> </ul> | Ninguno | N/C                                                                                                                                                                                                                                                                                                                                                                                            |
|                                                                              |                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                           |         |                                                                                                                                                                                                                                                                                                                                                                                                |

|                                                                                           |                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                   |                |
|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <p><b>Características generales:<br/>Operaciones en el Servidor de administración</b></p> | <ul style="list-style-type: none"> <li>• Leer</li> <li>• Escritura</li> <li>• Ejecutar</li> <li>• Modificar ACL de objeto</li> <li>• Realizar operaciones en selecciones de dispositivos</li> </ul> | <ul style="list-style-type: none"> <li>• Especificar puertos del Servidor de administración para la conexión del Agente de red:<br/><b>Escritura</b></li> <li>• Especificar los puertos del Proxy de activación que se está ejecutando en el Servidor de administración:<br/><b>Escritura</b></li> <li>• Especificar los puertos del Proxy de activación de dispositivos móviles que se está ejecutando en el Servidor de administración:<br/><b>Escritura</b></li> <li>• Especificar los puertos del Servidor web para la distribución de paquetes independientes:<br/><b>Escritura</b></li> <li>• Especificar los puertos del Servidor web para la distribución de perfiles MDM:<br/><b>Escritura</b></li> <li>• Especificar los puertos SSL del Servidor de administración para la conexión a través de Web Console:<br/><b>Escritura</b></li> <li>• Especificar puertos del Servidor de administración para conexión de dispositivos móviles:<br/><b>Escritura</b></li> <li>• Especificar el número máximo de eventos que pueden almacenar en la base</li> </ul> | <ul style="list-style-type: none"> <li>• "Copia de seguridad de los datos del Servidor de administración"</li> <li>• "Mantenimiento de bases de datos"</li> </ul> | <p>Ninguno</p> |
|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|

|                                                                                   |                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                       |         |                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                   |                                                                                                                                                                                                                            | <p>de datos del Servidor de administración:</p> <p><b>Escritura</b></p> <ul style="list-style-type: none"> <li>• Especificar el número máximo de eventos que el Servidor de administración puede enviar: <b>Escritura</b></li> <li>• Especificar el periodo de tiempo durante el cual el Servidor de administración puede enviar eventos: <b>Escritura</b></li> </ul> |         |                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <p><b>Características generales:</b><br/>Despliegue del software de Kaspersky</p> | <ul style="list-style-type: none"> <li>• <b>Administrar parches de Kaspersky</b></li> <li>• Leer</li> <li>• <b>Escritura</b></li> <li>• Ejecutar</li> <li>• Realizar operaciones en selecciones de dispositivos</li> </ul> | <p>Aprobar o rechazar la instalación del parche: <b>Administrar parches de Kaspersky</b></p>                                                                                                                                                                                                                                                                          | Ninguno | <ul style="list-style-type: none"> <li>• "Informe sobre el uso de claves de licencia por Servidor de administración virtual"</li> <li>• "Informe de versiones del software de Kaspersky"</li> <li>• "Informe de aplicaciones incompatibles"</li> <li>• "Informe sobre la versión de las actualizaciones para los módulos de software de Kaspersky"</li> <li>• "Informe del despliegue de la protección"</li> </ul> |
| <p><b>Características generales:</b><br/>Administración de claves</p>             | <ul style="list-style-type: none"> <li>• <b>Exportar archivo de clave</b></li> <li>• <b>Escritura</b></li> </ul>                                                                                                           | <ul style="list-style-type: none"> <li>• Exportar un archivo de clave: <b>Exportar archivo de clave</b></li> <li>• Modificar la configuración de la clave de licencia del</li> </ul>                                                                                                                                                                                  | Ninguno | N/C                                                                                                                                                                                                                                                                                                                                                                                                                |

|                                                                                               |                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |         |     |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-----|
|                                                                                               |                                                                                                                                                          | <p>Servidor de administración:<br/><b>Escritura</b></p>                                                                                                                                                                                                                                                                                                                                                                                           |         |     |
| <p><b>Características generales:</b><br/><b>Administración de informes</b></p>                | <ul style="list-style-type: none"> <li>• Leer</li> <li>• Escritura</li> </ul>                                                                            | <ul style="list-style-type: none"> <li>• Crear informes independientemente de sus ACL: <b>Escribir</b></li> <li>• Ejecutar informes independientemente de sus ACL: <b>Leer</b></li> </ul>                                                                                                                                                                                                                                                         | Ninguno | N/C |
| <p><b>Características generales:</b><br/><b>Jerarquía de Servidores de administración</b></p> | <p><b>Configurar los parámetros de jerarquía del Servidor de administración</b></p>                                                                      | <ul style="list-style-type: none"> <li>• Registrar, actualizar o eliminar Servidores de administración secundarios:<br/><b>Configurar la jerarquía de Servidores de administración</b></li> </ul>                                                                                                                                                                                                                                                 | Ninguno | N/C |
| <p><b>Características generales:</b><br/><b>Permisos de usuario</b></p>                       | <p><b>Modificar ACL de objeto</b></p>                                                                                                                    | <ul style="list-style-type: none"> <li>• Cambiar las propiedades de seguridad de cualquier objeto:<br/><b>Modificar ACL de objeto</b></li> <li>• Administrar roles de usuario: <b>Modificar ACL de objeto</b></li> <li>• Administrar usuarios internos: <b>Modificar ACL de objeto</b></li> <li>• Administrar grupos de seguridad:<br/><b>Modificar ACL de objeto</b></li> <li>• Administrar alias:<br/><b>Modificar ACL de objeto</b></li> </ul> | Ninguno | N/C |
| <p><b>Características generales:</b><br/><b>Servidores de administración virtuales</b></p>    | <ul style="list-style-type: none"> <li>• <b>Administración de Servidores de administración virtuales</b></li> <li>• Leer</li> <li>• Escritura</li> </ul> | <ul style="list-style-type: none"> <li>• Obtener la lista de Servidores de administración virtuales: <b>Leer</b></li> <li>• Obtener información sobre el Servidor de administración virtual: <b>Leer</b></li> </ul>                                                                                                                                                                                                                               | Ninguno | N/C |

|                                                                                 |                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                            |                                          |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
|                                                                                 | <ul style="list-style-type: none"> <li>• <b>Ejecutar</b></li> <li>• <b>Realizar operaciones en selecciones de dispositivos</b></li> </ul>                                                    | <ul style="list-style-type: none"> <li>• Crear, actualizar o eliminar un Servidor de administración virtual: <b>Administrar Servidores de administración virtuales</b></li> <li>• Mover un Servidor de administración virtual a otro grupo: <b>Administrar Servidores de administración virtuales</b></li> <li>• Definir los permisos de un Servidor de administración virtual: <b>Administrar Servidores de administración virtuales</b></li> </ul> |                                                                                                                                                            |                                          |
| <b>Características generales: Administración de claves de cifrado</b>           | <b>Escritura</b>                                                                                                                                                                             | Importar las claves de cifrado: <b>Escritura</b>                                                                                                                                                                                                                                                                                                                                                                                                     | Ninguno                                                                                                                                                    | N/C                                      |
| <b>Administración de sistemas: Administración de vulnerabilidades y parches</b> | <ul style="list-style-type: none"> <li>• <b>Leer</b></li> <li>• <b>Escritura</b></li> <li>• <b>Ejecutar</b></li> <li>• <b>Realizar operaciones en selecciones de dispositivos</b></li> </ul> | <ul style="list-style-type: none"> <li>• Ver propiedades de parches de terceros: <b>Leer</b></li> <li>• Cambiar las propiedades del parche de terceros: <b>Escritura</b></li> </ul>                                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>• "Reparar vulnerabilidades"</li> <li>• "Instalar actualizaciones requeridas y reparar vulnerabilidades"</li> </ul> | "Informe de actualizaciones de software" |

## Roles de usuario predefinidos

Las funciones de usuario asignadas a los usuarios de Kaspersky Security Center Linux les proporcionan conjuntos de derechos de acceso 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 y configurar los derechos necesarios por su cuenta. Algunas de las funciones de usuario predefinidas disponibles en Kaspersky Security Center Linux se pueden asociar con puestos de trabajo específicos, por ejemplo, **Auditor**, **Director de seguridad**, **Supervisor**. 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.

| Rol                  | Comentario                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auditor              | Permite realizar todas las operaciones con todos los tipos de informe, todas las operaciones de visualización, que incluye la visualización de objetos eliminados (con todos los permisos <b>Leer y Escribir</b> en el área <b>Objetos eliminados</b> ). No permite realizar otras operaciones. Puede asignar este rol a la persona que realiza la auditoría de su organización. |
| 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 <b>Administración de sistemas: Conectividad</b> . 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.

Las características de las áreas funcionales **Administración de dispositivos móviles: general** y **Administración del sistema** no están disponibles en Kaspersky Security Center Linux. Un usuario con las funciones **Administrador/operador de administración de parches y vulnerabilidades** o **Administrador/operador de administración de dispositivos móviles** tiene acceso solo por los derechos del área funcional **Características generales: Funcionalidad básica**.

## Derechos de acceso de los roles de usuario predefinidos

| Rol                                          | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrador del Servidor de administración | <p>Permite todas las operaciones en las siguientes áreas funcionales, en <b>Características generales</b>:</p> <ul style="list-style-type: none"> <li>• <b>Funcionalidad básica</b></li> <li>• <b>Procesamiento de eventos</b></li> <li>• <b>Jerarquía de Servidores de administración</b></li> <li>• <b>Servidores de administración virtuales</b></li> </ul> <p>Otorga los derechos de <b>lectura y escritura</b> en el área funcional <b>Características generales: Administración de claves de cifrado</b>.</p> |
| Operador del Servidor de administración      | <p>Otorga los derechos de <b>lectura y ejecución</b> en todas las áreas funcionales siguientes, en <b>Funciones generales</b>:</p> <ul style="list-style-type: none"> <li>• <b>Funcionalidad básica</b></li> <li>• <b>Servidores de administración virtuales</b></li> </ul>                                                                                                                                                                                                                                         |
| Auditor                                      | <p>Permite todas las operaciones en las siguientes áreas funcionales, en <b>Características generales</b>:</p> <ul style="list-style-type: none"> <li>• <b>Acceder a objetos sin importar sus ACL</b></li> <li>• <b>Objetos eliminados</b></li> <li>• <b>Administración de informes forzados</b></li> </ul> <p>Puede asignar este rol a la persona que realiza la auditoría de su organización.</p>                                                                                                                 |
|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



|                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Administrador de instalación</p>                 | <p>Permite todas las operaciones en las siguientes áreas funcionales, en <b>Características generales</b>:</p> <ul style="list-style-type: none"> <li>• <b>Funcionalidad básica</b></li> <li>• <b>Despliegue del software de Kaspersky</b></li> <li>• <b>Administración de claves de licencia</b></li> </ul> <p>Otorga derechos de <b>lectura</b> y <b>ejecución</b> en el área funcional <b>Características Generales: Servidores de administración Virtual</b>.</p>   |
| <p>Operador de instalación</p>                      | <p>Otorga los derechos de <b>lectura</b> y <b>ejecución</b> en todas las áreas funcionales siguientes, en <b>Funciones generales</b>:</p> <ul style="list-style-type: none"> <li>• <b>Funcionalidad básica</b></li> <li>• <b>Despliegue del software de Kaspersky</b> (también otorga el derecho <b>Administrar parches de Kaspersky</b> en esta área)</li> <li>• <b>Servidores de administración virtuales</b></li> </ul>                                              |
| <p>Administrador de Kaspersky Endpoint Security</p> | <p>Permite todas las operaciones en las siguientes áreas funcionales:</p> <ul style="list-style-type: none"> <li>• <b>Características generales: funcionalidad básica</b></li> <li>• <b>Área de Kaspersky Endpoint Security</b> (se incluyen todas las funciones)</li> </ul> <p>Otorga los derechos de <b>lectura</b> y <b>escritura</b> en el área funcional <b>Características generales: Administración de claves de cifrado</b>.</p>                                |
| <p>Operador de Kaspersky Endpoint Security</p>      | <p>Otorga los derechos <b>Leer</b> y <b>Ejecutar</b> en las siguientes áreas funcionales:</p> <ul style="list-style-type: none"> <li>• <b>Características generales: funcionalidad básica</b></li> <li>• <b>Área de Kaspersky Endpoint Security</b> (se incluyen todas las funciones)</li> </ul>                                                                                                                                                                        |
| <p>Administrador principal</p>                      | <p>Permite todas las operaciones en todas las áreas funcionales, <i>excepto</i> en las siguientes áreas, en <b>Características generales</b>:</p> <ul style="list-style-type: none"> <li>• <b>Acceder a objetos sin importar sus ACL</b></li> <li>• <b>Administración de informes forzados</b></li> </ul> <p>Otorga los derechos de <b>lectura</b> y <b>escritura</b> en el área funcional <b>Características generales: Administración de claves de cifrado</b>.</p>   |
| <p>Operador principal</p>                           | <p>Otorga los derechos <b>Leer</b> y <b>Ejecutar</b> (cuando corresponde) en las siguientes áreas funcionales:</p> <ul style="list-style-type: none"> <li>• <b>Características generales:</b></li> <li>• <b>Funcionalidad básica</b></li> <li>• <b>Objetos eliminados</b></li> <li>• <b>Operaciones en el Servidor de administración</b></li> <li>• <b>Despliegue del software de Kaspersky Lab</b></li> <li>• <b>Servidores de administración virtuales</b></li> </ul> |

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                         | <ul style="list-style-type: none"> <li>• Área de Kaspersky Endpoint Security (se incluyen todas las funciones)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Administrador de Administración de dispositivos móviles | Permite todas las operaciones en el área funcional <b>Características generales: Funcionalidad básica.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Director de seguridad                                   | <p>Permite todas las operaciones en las siguientes áreas funcionales, en <b>Características generales:</b></p> <ul style="list-style-type: none"> <li>• <b>Acceder a objetos sin importar sus ACL</b></li> <li>• <b>Administración de informes forzados</b></li> </ul> <p>Otorga derechos de <b>Lectura, Escritura, Ejecución, Guardar archivos desde los dispositivos a la estación de trabajo del administrador</b> y <b>Realizar operaciones para las selecciones de dispositivos</b> en el área funcional <b>Administración del sistema: Conectividad.</b></p> <p>Puede asignar este rol al responsable de la seguridad de TI de su organización.</p> |
| Usuario de Self Service Portal                          | Permite todas las operaciones en el área funcional <b>Administración de dispositivos móviles: Self Service Portal.</b> Esta función no es compatible con Kaspersky Security Center 11 ni versiones posteriores.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Supervisor                                              | <p>Otorga el derecho <b>Leer</b> en las áreas funcionales <b>Características generales: Acceder a objetos sin importar sus ACL</b> y <b>Características generales: Administración de informes controlada.</b></p> <p>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.</p>                                                                                                                                                                                                                                                                                                |

## 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**

- **Control e informes** → **Informes**
- **Activos (dispositivos)** → **Selecciones de dispositivos**
- **Control 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, active la opción **Usar permisos personalizados**.

5. Configure los derechos de acceso:

- Utilice los botones **Añadir** 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 una [función de usuario](#) al usuario o grupo de seguridad, seleccione el usuario o grupo de seguridad, haga clic en el botón **Funciones** y, a continuación, seleccione la función que desea asignar.

6. Haga clic en el botón **Guardar**.

Los derechos de acceso al objeto se configuran.

## Asignación de derechos de acceso a usuarios y grupos

Puede otorgar a los usuarios y a los grupos derechos de acceso para usar diferentes funciones del Servidor de administración y de las aplicaciones de Kaspersky para las cuales tiene complementos de administración, por ejemplo, Kaspersky Endpoint Security for Linux.

*Para asignar derechos de acceso a un usuario o un grupo de 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 **Derechos de acceso**, elija la casilla ubicada junto al nombre del usuario o el grupo de seguridad al que desee asignar derechos y, a continuación, haga clic en el botón **Derechos de acceso**.

No puede elegir varios usuarios o grupos de seguridad al mismo tiempo. Si selecciona más de un elemento, el botón **Derechos de acceso** se desactivará.

3. Configure el conjunto de derechos para el usuario o grupo:

a. Amplíe el nodo con funciones del Servidor de administración u otra aplicación de Kaspersky.

b. Seleccione la casilla **Permitir** o **Denegar** ubicada junto a la función o el derecho de acceso que desee.

*Ejemplo 1:* seleccione la casilla **Permitir** ubicada junto al nodo **Integración de la aplicación** para otorgar todos los derechos de acceso disponibles a la función Integración de la aplicación (**Lectura**, **Escritura** y **Ejecución**) para un usuario o grupo.

*Ejemplo 2:* expanda el nodo **Administración de claves de cifrado** y, a continuación, seleccione la casilla **Permitir** ubicada junto al permiso **Escritura** para otorgar el derecho de acceso **Escritura** a la función Administración de claves de cifrado para un usuario o grupo.

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:
  - Administración de grupos de administración (solo para Kaspersky Security Center Linux 11 o versiones posteriores)
  - Acceda a los objetos independientemente de sus ACL (solo para Kaspersky Security Center Linux 11 o versiones posteriores)
  - Funcionalidad básica
  - Objetos eliminados (solo para Kaspersky Security Center Linux 11 o versiones posteriores)
  - Administración de claves de cifrado
  - Procesamiento de eventos
  - Operaciones en el Servidor de administración (solo en la ventana de propiedades del Servidor de administración)
  - Despliegue del software de Kaspersky
  - Administración de claves de licencia
  - Integración de la aplicación
  - Administración de informes forzados
  - Jerarquía de Servidores de administración
  - Permisos de usuario
  - Servidores de administración virtuales
- Administración de dispositivos móviles:
  - General
  - Self Service Portal

- Administración de sistemas:
  - Conectividad
  - Inventario de hardware
  - Control de acceso a la red
  - Despliegue del sistema operativo
  - Instalación remota
  - Inventario de software

Si no se selecciona **Permitir** ni **Denegar** para un derecho de acceso, el derecho de acceso 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 todas las funciones asignadas a este usuario
- los derechos de todo el grupo de seguridad al que pertenece el usuario
- los derechos de todas las funciones asignadas 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.

## Agregar una cuenta de un usuario interno

*Para añadir una nueva cuenta de usuario interno a Kaspersky Security Center Linux:*

1. En el menú principal, vaya a **Usuarios y funciones** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en **Añadir**.
3. En la ventana **Añadir usuario** que se abre, especifique la configuración de la nueva cuenta de usuario:
  - **Nombre**.
  - **Contraseña** para la conexión del usuario a Kaspersky Security Center Linux.  
La contraseña debe cumplir con las siguientes reglas:
    - La contraseña debe tener entre 8 y 16 caracteres
    - La contraseña debe contener caracteres de al menos tres de los grupos enumerados a continuación:
      - Letras mayúsculas (A-Z)
      - Letras minúsculas (a-z)

- Números (0-9)
- Carácteres especiales (@ # \$ % ^ & \* - \_ ! + = [ ] { } | : ' . . ? / \ ` ~ " ( ) ;)
- La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@", cuando "." está colocado delante de "@".

Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

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. Puede desbloquear la cuenta de usuario solo cambiando la contraseña.

4. Haga clic en **Guardar** para guardar los cambios.

Se añade una nueva cuenta de usuarios a la lista de usuarios.

## Creación de un grupo de seguridad

*Para crear un grupo de seguridad, siga estos pasos:*

1. En el menú principal, vaya a **Usuarios y funciones** → **Usuarios y grupos** y luego seleccione la pestaña **Grupos**.
2. Haga clic en **Añadir**.
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 añade un nuevo grupo de seguridad a la lista de grupos.

## Editar una cuenta de un usuario interno

*Modificar una cuenta de usuario interna en Kaspersky Security Center Linux:*

1. En el menú principal, vaya a **Usuarios y funciones** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en el nombre de la cuenta de usuario que desea editar.

3. En la ventana de configuración de usuario que se abre, en la pestaña **General**, cambie la configuración de la cuenta de usuario:

- **Descripción**
- **Nombre completo**
- **Dirección de correo electrónico**
- **Teléfono principal**
- **Establecer contraseña nueva** para la conexión del usuario a Kaspersky Security Center Linux.

La contraseña debe cumplir con las siguientes reglas:

- La contraseña debe tener entre 8 y 16 caracteres
- La contraseña debe contener 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; sin embargo, por razones de seguridad, no recomendamos que reduzca este número. Si el usuario escribe una contraseña inválida el número de veces especificado, la cuenta de usuario se bloquea durante una hora. Puede desbloquear la cuenta de usuario solo cambiando la contraseña.

- Si es necesario, cambie el botón de alternar a **Desactivado** para prohibir que el usuario se conecte a la aplicación. Puede desactivar una cuenta, por ejemplo, después de que un empleado abandone la empresa.

4. En la pestaña **Seguridad de la 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 **Funciones**, puede [asignar funciones](#) al usuario.

8. Haga clic en **Guardar** para guardar los cambios.

La cuenta de usuario actualizada aparece en la lista de usuarios.

## Edición de un grupo de seguridad

*Para editar un grupo de seguridad, siga estos pasos:*

1. En el menú principal, vaya a **Usuarios y funciones** → **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**. Esta configuración solo está disponible para grupos de seguridad internos.
  - En la pestaña **Usuarios**, puede [añadir usuarios al grupo de seguridad](#). Esta configuración solo está disponible para usuarios internos y grupos de seguridad internos.
  - En la pestaña **Funciones**, 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 grupo de seguridad

*Para asignar una función a un usuario o grupo de seguridad, haga lo siguiente:*

1. En el menú principal, vaya a **Usuarios y funciones** → **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 una función.  
Puede seleccionar varios nombres.
3. En la línea del menú, haga clic en el botón **Asignar función**.  
Se inicia el Asistente de asignación de funciones.
4. Siga las instrucciones del asistente: seleccione la función que desea asignar a los usuarios o grupos de seguridad seleccionados, y luego seleccione el alcance de la función.

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.

La función 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 funciones asignadas**.

## Adición de cuentas de usuario a un grupo de seguridad interno



Solo puede añadir cuentas de usuarios internos a un grupo de seguridad interno.

*Para añadir cuentas de usuario a un grupo de seguridad interno, siga estos pasos:*

1. En el menú principal, vaya a **Usuarios y funciones** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Seleccione las casillas junto a las cuentas de usuario que desea añadir a un grupo de seguridad.
3. Haga clic en el botón **Asignar grupo**.
4. En la ventana que se abre **Asignar grupo**, seleccione el grupo de seguridad al que desea añadir cuentas de usuario.
5. Haga clic en el botón **Guardar**.

Las cuentas de usuario se añaden al grupo de seguridad. También puede añadir usuarios internos a un grupo de seguridad mediante la [configuración del grupo](#).

## Designación de un usuario como propietario de un dispositivo

Para obtener información sobre cómo asignar un usuario como propietario de un dispositivo móvil, consulte la [Ayuda de Kaspersky Security para dispositivos móviles](#) <sup>2</sup>.

*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 icono de flecha (▼) 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 funciones** → **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 los ajustes del usuario, seleccione la pestaña **Dispositivos**.
5. Haga clic en **Añadir**.
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**.

## 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 funciones** → **Usuarios y grupos** y luego seleccione la pestaña **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 **Seguridad de la autenticación**.
4. En la pestaña **Seguridad de la autenticación**, seleccione la opción **Solicitar autenticación para comprobar el permiso de modificación de esta cuenta** si desea solicitar credenciales cada vez que se cambia o modifica 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**.

## Verificación en dos pasos

En esta sección, se describe cómo puede utilizar la verificación en dos pasos para reducir el riesgo de que se ingrese sin autorización a Kaspersky Security Center Web Console.

## Escenario: configurar la verificación en dos pasos para todos los usuarios

Este escenario 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 escenario 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 derechos de Modificar ACL de objeto del área funcional **Funciones 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 Instalación de 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 Key
- Avanpost Authenticator
- Aladdin 2FA

Para comprobar si Kaspersky Security Center Linux es compatible con la aplicación de autenticación que desea utilizar, active la verificación en dos pasos para todos los usuarios o para un usuario en particular.

Uno de los pasos sugiere que especifique el código de seguridad generado por la aplicación de autenticación. Si tiene éxito, Kaspersky Security Center Linux será compatible con el autenticador seleccionado.

### 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 con la aplicación de autenticación y la hora del dispositivo con el Servidor de administración estén sincronizadas con UTC, mediante el uso de fuentes de hora 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

Después de [activar la verificación en dos pasos para su cuenta](#), puede activar la verificación en dos pasos para todos los usuarios.

### 4 Habilitación de la verificación en dos pasos para todos los usuarios

Los usuarios que tengan [activada la verificación en dos pasos](#) deben usarla para iniciar sesión en el Servidor de administración.

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

Para mejorar la seguridad del acceso a Kaspersky Security Center Web Console, puede [prohibirles a los nuevos usuarios configurar la verificación en dos pasos](#).

### 6 Editar el nombre del emisor de un código de seguridad

Si tiene varios Servidores de administración con nombres similares, [es posible que deba cambiar los nombres de los emisores del código de seguridad](#) para reconocer mejor los diferentes Servidores de administración.

## 7 Excluir las cuentas de usuario para las que no es necesario habilitar la verificación en dos pasos

Si es necesario, [puede excluir 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.

## 8 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 Web Console. De lo contrario, no podrán acceder al Servidor de administración de acuerdo con sus derechos.

## Resultados

Una vez completado este escenario:

- 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 de una cuenta

Kaspersky Security Center Linux proporciona verificación en dos pasos para los usuarios de Kaspersky Security Center Web Console. Cuando la verificación en dos pasos está activada para su propia cuenta, cada vez que inicie sesión en Kaspersky Security Center Web Console, debe introducir su nombre de usuario, contraseña y un código de seguridad adicional de un solo uso. Para recibir un código de seguridad de un solo uso, debe tener una app de autenticación en su ordenador o dispositivo móvil.

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 app de autenticación. Puede cambiar el nombre del emisor del código de seguridad. El nombre del emisor del código de seguridad tiene un valor predeterminado que es el mismo que el nombre del Servidor de administración. El nombre del emisor se utiliza como un identificador del Servidor de administración en la app de autenticación. Si cambia el nombre del emisor del código de seguridad, debe emitir una nueva clave secreta y pasarla a la app de autenticación. Los códigos de seguridad son de un solo uso y válidos por hasta 90 segundos (el tiempo exacto puede variar).

Cualquier usuario que tenga activada la verificación en dos pasos puede volver a emitir su propia clave secreta. Cuando un usuario se autentica con la clave secreta reemitida y la usa para iniciar sesión, el Servidor de administración guarda la nueva clave secreta de la cuenta de usuario. Si un usuario introduce la clave secreta de forma incorrecta al formulario de autenticación, el Servidor de administración no guarda la nueva clave secreta y conserva la validez de la clave secreta vigente para la autenticación posterior.

Cualquier software de autenticación que admita el algoritmo de contraseña de un solo uso basado en tiempo (TOTP) se puede utilizar como app de autenticación, por ejemplo, Google Authenticator. Para generar el código de seguridad, debe sincronizar la hora configurada en la app de autenticación con la hora configurada del Servidor de administración.

Para comprobar si Kaspersky Security Center Linux es compatible con la app de autenticación que desea utilizar, active la verificación en dos pasos para todos los usuarios o para un usuario en particular.

Uno de los pasos sugiere que especifique el código de seguridad generado por la app de autenticación. Si tiene éxito, Kaspersky Security Center Linux será compatible con el autenticador seleccionado.

Una app de autenticación genera el código de seguridad de la siguiente manera:

1. El Servidor de administración genera una clave secreta especial y un código QR.
2. Usted pasa la clave secreta generada o el código QR a la app de autenticación.
3. La app de autenticación genera un código de seguridad de un solo uso que usted debe ingresar en la ventana de autenticación del Servidor de administración.

Recomendamos que instale una app de autenticación en más de un dispositivo. Guarde la clave secreta (o el código QR) y consérvelos en un lugar seguro. Con esto, evitará quedar sin acceso a Kaspersky Security Center Web Console si no puede utilizar su dispositivo móvil.

Para proteger el uso de Kaspersky Security Center Linux, puede habilitar la verificación en dos pasos para su propia 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.

La verificación en dos pasos funciona según las siguientes reglas:

- Solo una cuenta de usuario que tenga los derechos Modificar objeto ACL en el área funcional **Funciones generales: Permisos de usuario** puede activar la verificación en dos pasos para todos los usuarios.
- Solo un usuario que haya habilitado la verificación en dos pasos para su propia cuenta puede habilitar la opción de verificación en dos pasos para todos los usuarios.
- Solo un usuario que haya habilitado la verificación en dos pasos para su propia cuenta puede excluir otras cuentas de usuario de la lista de verificación en dos pasos habilitada para todos los usuarios.
- Un usuario puede activar la verificación en dos pasos solo para su propia cuenta.
- Una cuenta de usuario que tiene el derecho Modificar las LCA de objetos en el área funcional **Características generales: permisos de usuario** y está conectado a Kaspersky Security Center Web Console mediante la verificación en dos pasos puede deshabilitar la verificación en dos pasos: a) para cualquier otro usuario solo si la verificación en dos pasos para todos los usuarios está deshabilitada; b) para un usuario excluido de la lista de verificación en dos pasos que esté habilitada para todos los usuarios.
- Cualquier usuario que haya iniciado sesión en Kaspersky Security Center Web Console mediante la verificación en dos pasos puede volver a emitir su clave secreta.
- Puede habilitar la opción de verificación en dos pasos para todos los usuarios para el Servidor de administración con el que está trabajando en un momento dado. Si activa esta opción en el Servidor de administración, también activa esta opción para las cuentas de usuario de sus [Servidores de administración virtuales](#) y no activa la verificación en dos pasos para las cuentas de usuario de los Servidores de administración secundarios.

## Habilitación de la verificación en dos pasos para su cuenta

Puede habilitar la verificación en dos pasos solo para su cuenta.

Antes de empezar a activar la verificación en dos pasos para su cuenta, asegúrese de que haya una aplicación de autenticación instalada en su dispositivo móvil. Asegúrese de que la hora establecida en la aplicación de autenticación esté sincronizada con la hora establecida del 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 funciones** → **Usuarios y grupos** y luego seleccione la pestaña **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 la 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 **Ver cómo configurar la verificación en dos pasos**.  
Ingrese la clave secreta en la aplicación de autenticación o haga clic en **Ver el 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 **Comprobar y aplicar**.
4. Haga clic en el botón **Guardar**.

La verificación en dos pasos está habilitada para su cuenta.

## Habilitación de la verificación en dos pasos para todos los usuarios

Puede activar la verificación en dos pasos para todos los usuarios del Servidor de administración si su cuenta tiene el derecho Modificar ACL de objetos en el área funcional **Funciones generales: Permisos de usuario** y si está autenticado mediante 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 la 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 **Ver cómo configurar la verificación en dos pasos**.

b. Ingrese la clave secreta en la aplicación de autenticación o haga clic en **Ver el 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 **Comprobar 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.

## Deshabilitar la verificación en dos pasos para una cuenta de usuario

Puede deshabilitar la verificación en dos pasos para su cuenta, así como para una cuenta de cualquier otro usuario.

Puede desactivar la verificación en dos pasos de la cuenta de otro usuario si su cuenta tiene el derecho Modificar LCA de objeto del área funcional **Características generales: Permisos de usuario**.

*Para deshabilitar la verificación en dos pasos para una cuenta de usuario, siga estos pasos:*

1. En el menú principal, vaya a **Usuarios y funciones** → **Usuarios y grupos** y luego seleccione la pestaña **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 **Seguridad de la autenticación**.
4. Seleccione la opción **Solicitar solo nombre de usuario y contraseña** si desea desactivar 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.

## Deshabilitar la verificación en dos pasos para todos los usuarios

Puede desactivar la verificación en dos pasos para todos los usuarios si la verificación en dos pasos está activada para su cuenta y su cuenta tiene el derecho Modificar LCA de objetos 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 la 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.

3. Ingrese las credenciales de su cuenta en la ventana de autenticación.

La verificación en dos pasos está inhabilitada para todos los usuarios.

## Excluir cuentas de la verificación en dos pasos

Puede excluir cuentas de usuario de la verificación en dos pasos si tiene el derecho Modificar LCA 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. 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 la autenticación** de la ventana de propiedades, en la tabla de exclusiones de la verificación en dos pasos haga clic en el botón **Añadir**.
3. 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.

## Configuración de la verificación en dos pasos para su cuenta

La primera vez que inicia sesión en Kaspersky Security Center Linux después de activar 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 aplicación de autenticación instalada en su dispositivo móvil. Asegúrese de que la hora del dispositivo con la aplicación de autenticación y la hora del dispositivo con el Servidor de administración estén sincronizadas con UTC, mediante el uso de fuentes de hora externas.

*Para configurar la verificación en dos pasos para su cuenta, siga estos pasos:*

1. Genere un código de seguridad único mediante la aplicación de autenticación en su dispositivo móvil. Para hacerlo, realice una de las siguientes acciones:
  - Introduzca la clave secreta en la aplicación de autenticación manualmente.



- Haga clic en **Ver el código QR** y escanee el código QR con la aplicación de autenticación.

Aparecerá un código de seguridad en su dispositivo móvil.

2. 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 **Comprobar y aplicar**.

La verificación en dos pasos se configura para su cuenta. Puede acceder al Servidor de administración de acuerdo con sus derechos.

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

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

Si esta opción está activada, un usuario con la verificación en dos pasos desactivada, 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 Linux que ya tenga activada la verificación en dos pasos.

Esta opción está disponible si [la verificación en dos pasos está activada para todos los usuarios](#).

*Para prohibir que los nuevos usuarios configuren la verificación en dos pasos por sí mismos, 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 la autenticación** de la ventana de propiedades, cambie el botón de activación **Prohibir a los nuevos usuarios configurar la verificación en dos pasos por sí mismos** a la posición activada.

Esta opción no afecta las cuentas de usuario añadidas 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 desactivada, desactive temporalmente la opción **Prohibir a los nuevos usuarios configurar la verificación en dos pasos por sí mismos**, solicite al usuario que active la verificación en dos pasos y, a continuación, vuelva a activar la opción.

## 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 funciones** → **Usuarios y grupos** y luego seleccione la pestaña **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 **Seguridad de la autenticación**.

4. En la pestaña **Seguridad de la autenticación**, haga clic en el vínculo **Generar una nueva clave secreta**.
5. En la ventana de verificación en dos pasos que se abre, especifique una nueva clave de seguridad generada por la aplicación de autenticación.
6. Haga clic en el botón **Comprobar y aplicar**.

Se genera una nueva clave secreta para el usuario.

Si pierde su dispositivo móvil, puede instalar una aplicación de autenticación en otro dispositivo móvil y generar una nueva clave secreta para restaurar el acceso a Kaspersky Security Center Web Console.

## Editar el nombre del emisor de un código de seguridad

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.

Después de cambiar el nombre del emisor del código de seguridad, hay que volver a emitir una nueva clave secreta y pasarla 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 **Seguridad de la autenticación**.
3. En la pestaña **Seguridad de la autenticación**, haga clic en el enlace **Editar**.  
Se abre la sección **Editar emisor de 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.

## Cambiar el número de intentos de entrada de contraseña permitidos

El usuario de Kaspersky Security Center Linux 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. En el dispositivo del Servidor de administración, ejecute una línea de comando de Linux.

2. Para la utilidad klscflag, ejecute el siguiente comando:

```
sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSp1PpcLogonAttempts -t d -v N
```

donde N es el número de intentos para ingresar una contraseña.

3. Para aplicar los cambios, reinicie el servicio del Servidor de administración.

Se cambia el número máximo de intentos de entrada de contraseña permitidos.

## 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 funciones** → **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 **Correcto**.

Se elimina el usuario o el grupo de seguridad.

## Creación de roles de usuario

*Para crear un rol de usuario:*

1. En el menú principal, vaya a **Usuarios y funciones** → **Funciones**.

2. Haga clic en **Añadir**.

3. En la ventana **Nombre de la nueva función** que se abre, introduzca el nombre del nuevo rol.

4. Haga clic en **Correcto** 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 funciones** → **Funciones**.
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 funciones** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios** o **Grupos**.
2. Active las casillas ubicadas junto a los usuarios o grupos de seguridad que desee añadir al alcance de la función de usuario.
3. Haga clic en el botón **Asignar función**.  
Se inicia el Asistente de asignación de funciones. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
4. En la página del asistente **Seleccionar función**, seleccione la función de usuario que quiere asignar.

5. En la página del asistente **Definir cobertura**, seleccione el grupo de administración que desea añadir a la cobertura de la función de usuario.

6. Haga clic en el botón **Asignar función** 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 funciones** → **Funciones**.

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 **Cobertura de la función**, haga clic en **Añadir**.

Se inicia el Asistente de asignación de funciones. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

5. En la página del asistente **Definir cobertura**, seleccione el grupo de administración que desea añadir a la cobertura de la función de usuario.

6. En la página del asistente **Seleccionar usuarios**, seleccione el grupo de seguridad y usuarios que desea añadir a la cobertura de la función de usuario.

7. Haga clic en el botón **Asignar función** para cerrar la ventana.

8. Haga clic en el botón **Cerrar** (X) para cerrar la ventana de propiedades de la función.

Los usuarios o grupos de seguridad y el grupo de administración 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 funciones** → **Funciones**.

2. Active la casilla de verificación ubicada junto al nombre del rol que desee eliminar.

3. Haga clic en **Eliminar**.

4. En la ventana que se abre, haga clic en **Correcto**.

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 funciones** → **Funciones**.
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. Active la casilla de verificación 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. Active la casilla de verificación adyacente al nuevo perfil.
6. Haga clic en **Asignar a función**.

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.

# 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
- Aplicaciones instaladas de Kaspersky, incluidos los componentes de Kaspersky Security Center Linux y las aplicaciones de seguridad

## Escenario: 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
- Aplicaciones instaladas de Kaspersky, incluidos los componentes de Kaspersky Security Center Linux y las aplicaciones de seguridad

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 Linux 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 y los módulos de software de Kaspersky de forma manual](#) o [directamente 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. Desplegado las aplicaciones de seguridad de Kaspersky en los dispositivos administrados según el [escenario de implementación de aplicaciones de Kaspersky a través de Kaspersky Security Center Web Console](#).
2. Creado y configurado todas las directivas, perfiles de directivas y tareas requeridas de acuerdo con el [escenario de configuración de 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

Puede usar [varios esquemas](#) para instalar actualizaciones en 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 es necesaria para descargar actualizaciones de los servidores de actualización de Kaspersky al repositorio del Servidor de administración, así como para actualizar las bases de datos y módulos de software de Kaspersky para Kaspersky Security Center Linux. 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: [Crear 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 transfieren del Servidor de administración a los puntos de distribución. Puede configurar Kaspersky Security Center Linux 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 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: [Creación de la tarea para descargar actualizaciones en los repositorios de los puntos de distribución](#)

### 4 Configurar los puntos de distribución

Cuando su red tenga puntos de distribución asignados, asegúrese de que la opción **Desplegar actualizaciones** esté habilitada en las propiedades de todos los puntos de distribución requeridos. 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.

### 5 Optimización del proceso de actualización mediante el uso de archivos diff (opcional)

Puede optimizar el tráfico entre el Servidor de administración y los dispositivos administrados utilizando [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, active la opción **Descargar archivos de comparación** en las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y/o la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*.

Instrucciones: [Uso de archivos diff para actualizar las bases de datos y módulos de software de Kaspersky](#)

### 6 Configurar la instalación automática de actualizaciones para las aplicaciones de seguridad



Cree las tareas de *Actualización* para las aplicaciones administradas a fin de proporcionar actualizaciones oportunas a los módulos de software y las bases de datos de Kaspersky, incluidas las bases de datos antivirus. Para garantizar actualizaciones oportunas, le recomendamos que seleccione la opción **Cuando se descarguen nuevas actualizaciones en el repositorio** al [configurar la programación de tareas](#).

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 y el Agente de red 13.2 estén instalados en los dispositivos administrados.

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.

## Resultados

Una vez completado el escenario, Kaspersky Security Center Linux queda configurado para actualizar las bases de datos de Kaspersky después de que las actualizaciones se descargan en el repositorio del Servidor de administración. 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 Linux comprueba si se puede acceder a los servidores de Kaspersky. Si no es posible acceder a los servidores mediante el DNS del sistema, la aplicación utiliza [servidores de 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.

- Aplicaciones instaladas de Kaspersky, incluidos los componentes de Kaspersky Security Center Linux y las aplicaciones de seguridad

Kaspersky Security Center Linux no puede actualizar las aplicaciones de Kaspersky automáticamente. Para actualizar las aplicaciones, descargue las últimas versiones de las aplicaciones desde el sitio web de Kaspersky e instálelas manualmente:

- [Servidor de administración de Kaspersky Security Center Linux, Kaspersky Security Center Web Console](#) <sup>14</sup>
- [Agente de red, Kaspersky Endpoint Security, complemento web de administración](#) <sup>14</sup>

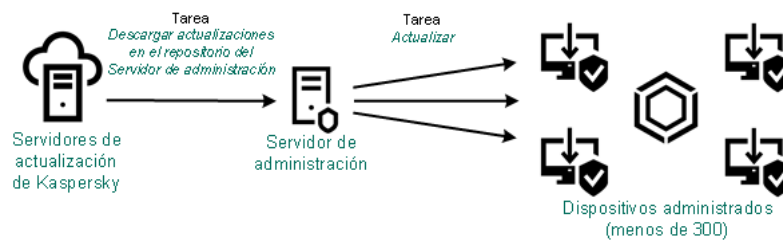
Existen distintos esquemas para descargar las actualizaciones necesarias y distribuirlas a los dispositivos administrados. La elección de una u otra opción depende de la configuración de la red. Estas son las posibilidades:

- Mediante el uso de 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 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 Linux descarga 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).



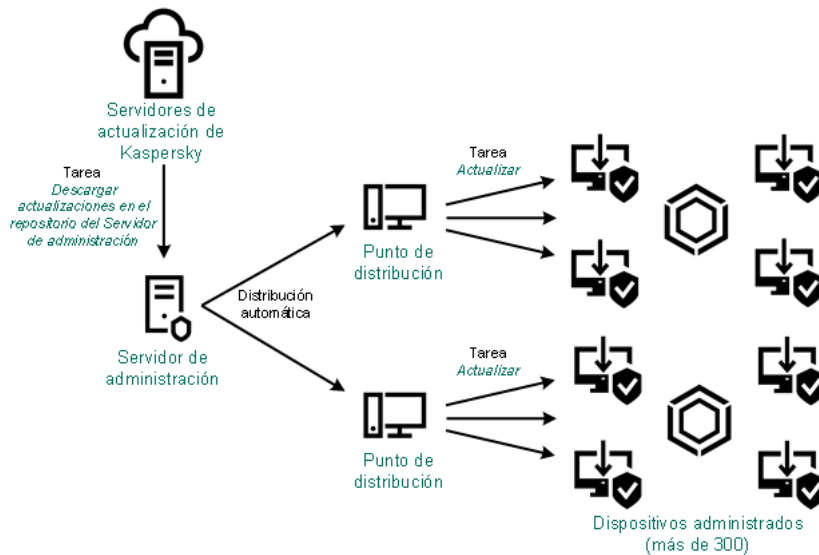
Actualización utilizando la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* sin puntos de distribución

Como [fuente de actualizaciones](#), no solo puede usar los servidores de actualización de Kaspersky, sino también una carpeta local o de red.

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 300 o más dispositivos administrados en un solo segmento de red o si su red consta de varios segmentos de red con más de 9 dispositivos administrados en cada segmento de red, le recomendamos que utilice [puntos de distribución](#) para propagar las actualizaciones a los dispositivos administrados (ver la siguiente figura). 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 utilizando la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* con puntos de distribución

Cuando se completa la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, las actualizaciones de las bases de datos de Kaspersky y los módulos de software para Kaspersky Endpoint Security se descargan en el repositorio del Servidor de administración. Estas actualizaciones se instalan a través de la tarea *Actualizar* de Kaspersky Endpoint Security.

La tarea *descargar actualizaciones en el repositorio del Servidor de administración* no está disponible en los 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.

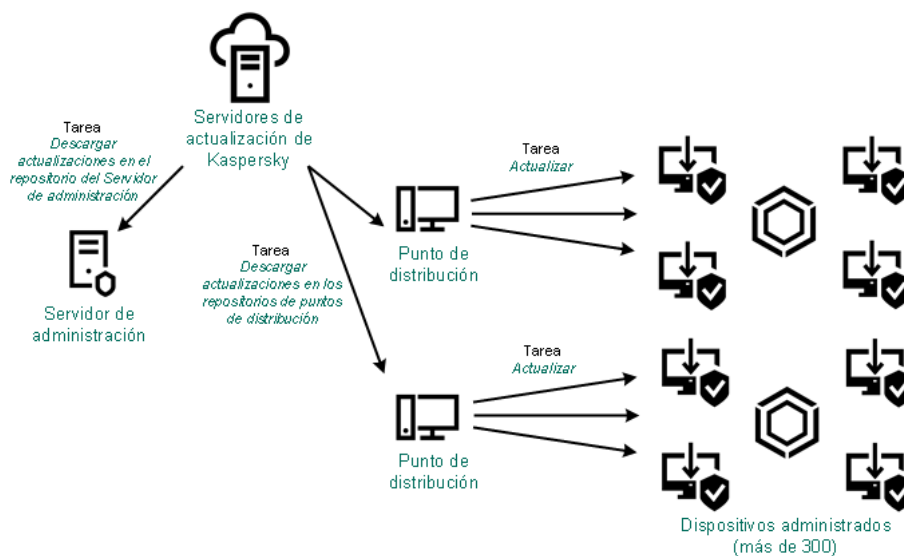
Cada aplicación de Kaspersky le solicita al Servidor de administración las actualizaciones que requiere. El Servidor de administración combina las solicitudes y descarga solo aquellas actualizaciones que han sido solicitadas por alguna aplicación. De este modo, se evita descargar la misma actualización 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 aplicaciones
- 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 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 utilizando la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*

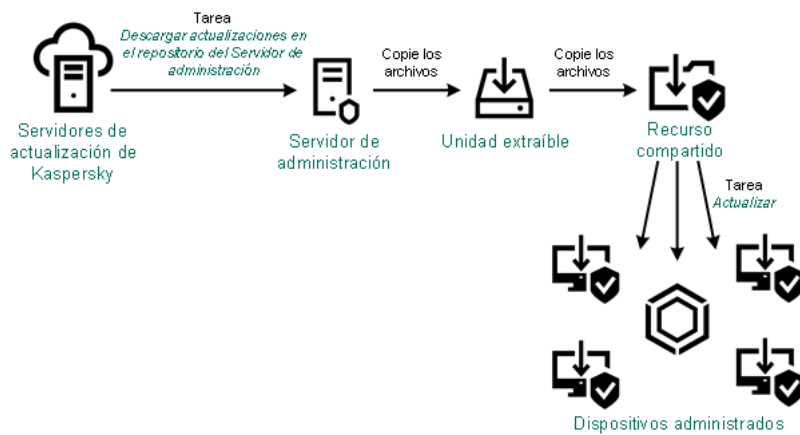
De forma predeterminada, el Servidor de administración y los puntos de distribución se comunican con los servidores de actualizaciones de Kaspersky y descargan las actualizaciones utilizando el protocolo HTTPS. Puede hacer que el Servidor de administración y/o los puntos de distribución utilicen el protocolo HTTP en lugar del protocolo HTTPS.

Para implementar este esquema, cree la tarea *Descargar actualizaciones en los repositorios de 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.

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* también es necesaria para este esquema, ya que esta tarea se utiliza para descargar las bases de datos y los módulos de software de Kaspersky para Kaspersky Security Center Linux.

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).



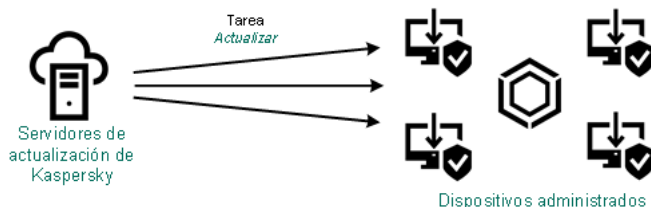
Actualización con una carpeta local, una carpeta compartida o un servidor FTP

Para obtener más información sobre los orígenes de actualizaciones en Kaspersky Endpoint Security, consulte los siguientes documentos de ayuda:

- [Ayuda de Kaspersky Endpoint Security for Linux](#)
- [Ayuda de Kaspersky Endpoint Security para Windows](#)

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 el repositorio proporcionado por Kaspersky Security Center Linux. Para recibir actualizaciones directamente de los servidores de actualización de Kaspersky, especifique los servidores de actualización de Kaspersky como origen de actualizaciones en la aplicación de seguridad. Para obtener más información acerca de estos ajustes, consulte los siguientes documentos de ayuda:

- [Ayuda de Kaspersky Endpoint Security for Linux](#)
- [Ayuda de Kaspersky Endpoint Security para Windows](#)

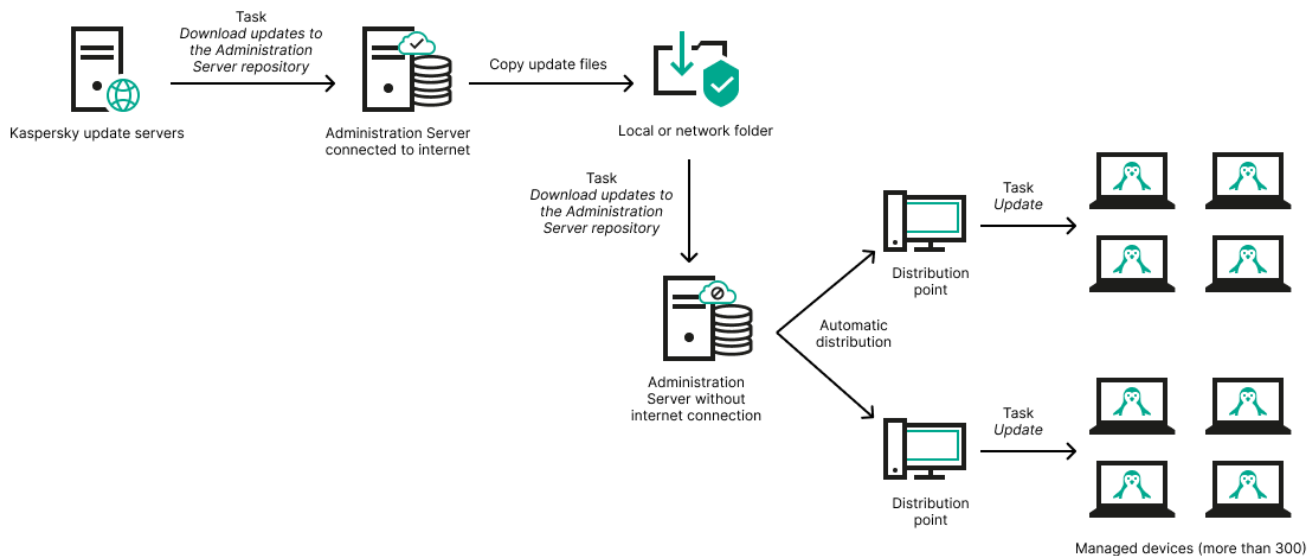
Utilizar una carpeta local o de red si el Servidor de administración no tiene conexión a Internet

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 actualizaciones utilizando 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 actualizaciones utilizando 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* permite descargar las actualizaciones de las bases de datos y los módulos de software para las aplicaciones de seguridad de Kaspersky desde los servidores de actualización de Kaspersky al repositorio del Servidor de Administración.

El asistente de inicio rápido de Kaspersky Security Center [crea automáticamente](#) la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* del Servidor de administración. En la lista de tareas, solo puede existir una tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Puede volver a crear esta tarea si se la ha eliminado de la lista de tareas del Servidor de administración.

Una vez finalizada la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* y descargadas las actualizaciones, se las puede propagar a los dispositivos administrados.

Antes de distribuir actualizaciones a los dispositivos administrados, puede ejecutar la tarea [Actualizar verificación](#). Esto le permite asegurarse de que el Servidor de administración instalará las actualizaciones descargadas correctamente y 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 **Añadir**.  
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. En la página **Finalizar la creación de tareas**, puede habilitar la opción **Abrir los detalles de la tarea cuando se complete la creación** para abrir la ventana de propiedades de la tarea y modificar la configuración predeterminada de la tarea. De lo contrario, puede configurar los ajustes de la tarea más tarde, en cualquier momento.
6. Haga clic en el botón **Finalizar**.  
La tarea se crea y se muestra en la lista de tareas.
7. Haga clic en el nombre de la tarea creada para abrir su ventana de propiedades.
8. En la ventana de propiedades de la tarea, en la pestaña **Configuración de la aplicación**, especifique la siguiente configuración:

- **[Orígenes de actualizaciones](#)** ⓘ

Puede usar como [origen de actualizaciones](#), los servidores de actualización de Kaspersky, una carpeta local o de red, o un Servidor de administración principal.

En la tarea *Descargar actualizaciones al repositorio del Servidor de administración* y la tarea *Descargar actualizaciones a los repositorios de los puntos de distribución*, la autenticación de usuario no funciona si selecciona como fuente de actualización una carpeta local o de red protegida con contraseña. Para resolver este problema, primero monte la carpeta protegida con contraseña y luego especifique las credenciales requeridas, por ejemplo, mediante el sistema operativo. Después, puede seleccionar esta carpeta como fuente de actualización en una tarea de descarga de actualización. Kaspersky Security Center Linux no requerirá que ingrese las credenciales.

- **[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.

- **[Forzar actualización en 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. 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 manera predeterminada.



- [Copiar las actualizaciones descargadas en 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.

Esta opción está deshabilitada de manera predeterminada.

- [Descargar archivos de comparación](#) 

Esta opción habilita la función de [descarga de archivos diff](#).

Esta opción está deshabilitada de manera predeterminada.

- [Descargar actualizaciones utilizando el esquema anterior](#) 

A partir de la versión 14, Kaspersky Security Center Linux descarga las actualizaciones de bases de datos y los módulos de software utilizando el nuevo esquema. 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 Linux

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 Servidor de administración 2 tiene la versión 13, active la opción **Descargar actualizaciones utilizando el esquema anterior** en la tarea para el Servidor de administración 1.

Esta opción está deshabilitada de manera 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 **Cuando se descargan nuevas actualizaciones en el 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 manera 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:

- **Inicio programado:**

- **Manualmente**  (seleccionado de manera predeterminada)

La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.  
Esta opción está habilitada de manera 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 forma predeterminada, la tarea se ejecutará cada seis 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.

- **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. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center Linux.

De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

- **Semanalmente** ⓘ

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 p. m.

- **Mensualmente** ⓘ

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 días concretos de las semanas seleccionadas** ⓘ

La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es a las 6:00:00 p. m.

- **Al completar otra tarea** ⓘ

La tarea actual se iniciará después de que se complete otra tarea. Puede seleccionar cómo se deberá completar esa tarea anterior (correctamente o con errores) para que se dé inicio a la tarea subsiguiente. Este parámetro solo funciona si ambas tareas están asignadas a los mismos dispositivos.

- Ajustes adicionales 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 **Manualmente, 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 se ejecutarán las tareas programadas en los dispositivos cliente; las tareas con las opciones de programación **Manualmente, Una vez e Inmediatamente** solo se ejecutarán en aquellos dispositivos cliente que estén 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 habilitada de manera predeterminada.

- [Usar el retraso aleatorio automáticamente 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.

- [Usar el retraso aleatorio para el inicio de tareas con un intervalo de \(min\)](#) 

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 manera predeterminada. El intervalo de tiempo predeterminado es de un minuto.

- [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 manera 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 **Cuando se descargan nuevas actualizaciones en el 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 de malware](#) para una aplicación compatible con Kaspersky Security Center Linux, por ejemplo, Kaspersky Endpoint Security for Linux. Al crear las tareas de actualización y análisis

de malware, especifique el grupo de administración con los dispositivos de prueba.

La tarea *Actualizar verificación* ejecuta secuencialmente las tareas de actualización y análisis de malware en los dispositivos de prueba para verificar que todas las actualizaciones sean válidas. Además, al crear la tarea *Actualizar verificación* debe especificar las tareas de actualización y análisis de malware.

3. Cree la tarea [Descargar actualizaciones en el repositorio del Servidor de administración](#).

Para que Kaspersky Security Center Linux 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 requerida compatible con Kaspersky Security Center Linux y luego seleccione la tarea de análisis de malware.

Hecho esto, aparecerán las siguientes opciones. Recomendamos que las deje habilitadas.

- [Reiniciar dispositivo después de actualizar 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 tras la actualización de las bases de datos y el reinicio del 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 habilitada de manera 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.

## Crear una tarea para descargar las actualizaciones en los repositorios de los puntos de distribución

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.

*Para crear la tarea **Descargar actualizaciones en los repositorios de puntos de distribución** para un grupo de administración específico:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en el botón **Añadir**.  
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 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 tareas**, 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 manera 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. Solo se puede usar un recurso compartido SMB montado como carpeta de red. La carpeta local debe ser una carpeta del dispositivo en el que se encuentra instalado el Servidor de administración.

En la tarea *Descargar actualizaciones al repositorio del Servidor de administración* y la tarea *Descargar actualizaciones a los repositorios de los puntos de distribución*, la autenticación de usuario no funciona si selecciona como fuente de actualización una carpeta local o de red protegida con contraseña. Para resolver este problema, primero monte la carpeta protegida con contraseña y luego especifique las credenciales requeridas, por ejemplo, mediante el sistema operativo. Después, puede seleccionar esta carpeta como fuente de actualización en una tarea de descarga de actualización. Kaspersky Security Center Linux no requerirá que ingrese las credenciales.

- **[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 de comparación](#)** 

Esta opción habilita la función de [descarga de archivos diff](#).  
Esta opción está deshabilitada de manera predeterminada.

- **[Descargar actualizaciones utilizando el esquema anterior](#)** 

A partir de la versión 14, Kaspersky Security Center Linux descarga las actualizaciones de bases de datos y los módulos de software utilizando el nuevo esquema. 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 Linux

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 tiene la versión 13, active la opción **Descargar actualizaciones utilizando el esquema anterior** en la tarea *Descargar actualizaciones a los repositorios de los puntos de distribución*.

Esta opción está deshabilitada de manera predeterminada.

10. Programe la ejecución de la tarea. De ser necesario, configure los siguientes ajustes:

- **Inicio programado:**

- [Manualmente](#)  (seleccionado de manera predeterminada)

La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.  
Esta opción está habilitada de manera 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 forma predeterminada, la tarea se ejecutará cada seis 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.

- **[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. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center Linux.

De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

- **[Semanalmente](#)** 

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 p. m.

- **[Mensualmente](#)** 

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 días concretos de las semanas seleccionadas](#)** 

La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es a las 6:00:00 p. m.

- **[Al detectar un foco 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 antivirus que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- [Al completar otra tarea](#)

La tarea actual se iniciará después de que se complete otra tarea. Puede seleccionar cómo se deberá completar esa tarea anterior (correctamente o con errores) para que se dé inicio a la tarea subsiguiente. Este parámetro solo funciona si ambas tareas están asignadas a los mismos dispositivos.

- [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 **Manualmente**, **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 se ejecutarán las tareas programadas en los dispositivos cliente; las tareas con las opciones de programación **Manualmente**, **Una vez** e **Inmediatamente** solo se ejecutarán en aquellos dispositivos cliente que estén 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 habilitada de manera predeterminada.

- [Usar el retraso aleatorio automáticamente 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.

- [Usar el retraso aleatorio para el inicio de tareas con un intervalo de \(min\)](#)

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 manera 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 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.

## Adición de fuentes de actualizaciones para la tarea Descargar actualizaciones al repositorio del Servidor de administración

Al crear o usar la [tarea para descargar actualizaciones al repositorio del Servidor de administración](#), puede elegir las siguientes fuentes de actualizaciones:

- Servidores de actualizaciones de Kaspersky
- 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

En la tarea *Descargar actualizaciones al repositorio del Servidor de administración* y la tarea *Descargar actualizaciones a los repositorios de los puntos de distribución*, la autenticación de usuario no funciona si selecciona como fuente de actualización una carpeta local o de red protegida con contraseña. Para resolver este problema, primero monte la carpeta protegida con contraseña y luego especifique las credenciales requeridas, por ejemplo, mediante el sistema operativo. Después, puede seleccionar esta carpeta como fuente de actualización en una tarea de descarga de actualización. Kaspersky Security Center Linux no requerirá que ingrese las credenciales.

Los servidores de actualización de Kaspersky se utilizan de forma predeterminada, pero también puede descargar actualizaciones desde una carpeta local o de red. Es posible que desee utilizar la carpeta si su red no tiene acceso a Internet. En este caso, puede descargar manualmente las actualizaciones de los servidores de actualización de Kaspersky y poner los archivos descargados en la carpeta necesaria.

Puede especificar solo una ruta a una carpeta local o de red. Como carpeta local, debe especificar una carpeta en el dispositivo en el que se encuentra instalado el Servidor de administración. Como carpeta de red, puede usar un servidor FTP o HTTP, o un recurso compartido SMB. Si un recurso compartido SMB requiere autenticación, se debe montar en el sistema con las credenciales requeridas de antemano. Recomendamos no utilizar el protocolo SMB1 ya que no es seguro.

Si añade los servidores de actualización de Kaspersky y la carpeta local o de red, las actualizaciones se descargarán primero desde la carpeta. En caso de error durante la descarga, se utilizarán los servidores de actualización de Kaspersky.

En caso de que una carpeta compartida que contenga actualizaciones esté protegida con contraseña, habilite la opción **Especificar cuenta para el acceso a la carpeta compartida del origen de actualizaciones (si la hay)** e ingrese las credenciales de cuenta requeridas para el acceso.

*Para añadir los orígenes de actualizaciones:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Descargar actualizaciones en el repositorio del Servidor de administración**.
3. Vaya a la pestaña **Configuración de la aplicación**.
4. En la línea **Orígenes de actualizaciones**, haga clic en el botón **Configurar**.
5. En la ventana que se abre, haga clic en el botón **Añadir**.
6. En la lista de orígenes de actualización, añada los orígenes necesarios. Si marca la casilla **Carpeta local o de red**, especifique una ruta a la carpeta.
7. Haga clic en **Aceptar** y, a continuación, cierre la ventana de propiedades del origen de actualizaciones.
8. En la ventana de orígenes de actualizaciones haga clic en **Aceptar**.
9. Haga clic en el botón **Guardar** en la ventana de la tarea.

Ahora las actualizaciones se descargan al repositorio del Servidor de administración desde las fuentes especificadas.

## Acerca de la utilización de archivos diff para actualizar las bases de datos y los módulos de software de Kaspersky

Cuando Kaspersky Security Center Linux 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.

Los puntos de distribución no utilizan la multidifusión IP para la distribución automática de archivos diff.

## Activación de la función de descarga de archivos diff: escenario

### Etapas

#### 1 Habilitar la función en el Servidor de administración

Active la función en la configuración de una tarea [Descargar de actualizaciones en el repositorio del Servidor de administración](#).

#### 2 Habilite la función para un punto de distribución

Active 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, active la función en la [configuración de la directiva del Agente de red](#) para un punto de distribución que reciba actualizaciones del servidor de administración.

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.

## Descarga de actualizaciones por puntos de distribución

Kaspersky Security Center Linux permite que los puntos de distribución reciban actualizaciones del Servidor de administración, de los servidores de Kaspersky o de una carpeta local o en red.

*Para configurar la descarga de actualizaciones para 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 a través del cual se enviarán las actualizaciones a los dispositivos cliente del grupo.
4. En la ventana de propiedades del punto de distribución, seleccione la sección **Origen de actualizaciones**.
5. Seleccione un origen de actualizaciones para el punto de distribución:

- [Origen de actualizaciones](#) 

Seleccione un origen de actualizaciones para el punto de distribución:

- Seleccione **Descargar del Servidor de administración** para que el punto de distribución pueda recibir actualizaciones del Servidor de administración.
- Seleccione **Utilizar la 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 una tarea** para crearla. Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

- [Descargar archivos de comparación](#) 

Esta opción habilita la función de [descarga de archivos diff](#).

Esta opción está habilitada de manera predeterminada.

El punto de distribución recibirá actualizaciones del origen especificado.

## 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.

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 mediante 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 Linux para copiar regularmente las actualizaciones a la carpeta que seleccione. Para ello, utilice la opción **Copiar las actualizaciones descargadas en carpetas adicionales** en las propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. 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 desconectados, configure Kaspersky Endpoint Security para recibir actualizaciones de una carpeta local o un recurso compartido, como un servidor FTP o una carpeta compartida.

Instrucciones:

- [Ayuda de Kaspersky Endpoint Security for Linux](#) <sup>12</sup>
- [Ayuda de Kaspersky Endpoint Security para Windows](#) <sup>12</sup>

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 desconectado que requiere la instalación de la actualización, inicie la tarea *Actualizar* de Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security para Windows, según el sistema operativo del dispositivo desconectado.

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 **Restaurar desde la copia de seguridad**.

El complemento web se restaura a partir de la copia de seguridad seleccionada.



# Supervisión, generación de informes y auditoría

Esta sección describe las capacidades de supervisión e informes de Kaspersky Security Center Linux. 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 Linux o durante su operación, puede configurar las funciones de supervisión e informes para que se adapten mejor a sus necesidades.

## Escenario: Supervisión y generación de informes

Esta sección proporciona un escenario para configurar la función Supervisión e informes en Kaspersky Security Center Linux.

### Requisitos previos

Después de desplegar Kaspersky Security Center Linux en la red de una organización, puede comenzar a supervisarlos y generar informes sobre su funcionamiento.

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 Realización de acciones recomendadas para notificaciones críticas, de advertencia e informativas

Instrucciones:

[Realizar acciones recomendadas para la red de su organización](#)

#### 4 Controlar el estado de seguridad de la red de la organización

Instrucciones:

- [Revisión del widget Estado de la protección](#)
- [Generación y revisión del Informe del estado de la protección](#)
- [Genere y revise el Informe de errores](#)

#### 5 Buscar dispositivos cliente que no se encuentren protegidos

Instrucciones:

- [Revise el widget Nuevos dispositivos](#)
- [Genere y revise el Informe del despliegue de la protección](#)

## 6 Controlar la protección de los dispositivos cliente

Instrucciones:

- [Generación y revisión de informes de las categorías Estado de la protección y Estadísticas de amenazas](#)
- [Inicie y revise la selección de eventos Crítico](#)

## 7 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:

- [Limitar el número máximo de eventos](#)

## 8 Controlar la información de las licencias

Instrucciones:

- [Añadir el widget Uso de claves 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, Fallos operativos, Advertencias y Eventos de información**
- Por fecha: **Eventos recientes**
- Por tipo: **Solicitudes de los usuarios 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 **Control 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 la protección
- Despliegue
- Actualización
- Estadísticas de amenazas
- Otro

Algunos widgets tienen información textual 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 **Control e informes** → **Panel**.

2. Haga clic en el botón **Añadir o restaurar un 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 **Añadir**.

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 **Control e informes** → **Panel**.

2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee ocultar.

3. Seleccione **Ocultar el 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 **Control 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 **Control 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 (gráfico 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 **Control 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:

- **Cobertura 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.
- **Asignar estado Crítico si se especifica lo siguiente y Asignar estado Advertencia si se especifica lo siguiente**: las reglas que determinan el color de un semáforo.

Después de cambiar la configuración del widget, puede actualizar los datos del widget manualmente.

*Para actualizar datos en un widget:*

1. En el menú principal, vaya a **Control 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 los empleados que no administran la red pero que desean ver las estadísticas de protección de la red en Kaspersky Security Center Linux (por ejemplo, un alto directivo). 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 un administrador del sistema, un proveedor de servicios administrados (MSP) o un usuario que tenga el derecho [Modificar ACL de objetos](#) el área funcional **Características generales: Permisos de usuario**.

## Configuración del modo solo panel

Antes de comenzar el [Modo Solo panel](#), asegúrese de que se cumplan los siguientes requisitos previos:

- Tiene el derecho [Modificar ACL de objetos](#) en el área funcional **Funciones generales: Permisos de usuario**. Si no tiene este derecho, no encontrará la pestaña para configurar el modo.
- El usuario tiene el derecho de [Lectura](#) en el área funcional **Funciones generales: Funcionalidad básica**.

Si se organiza una jerarquía de Servidores de administración en su red para configurar el modo de solo panel, vaya al Servidor donde la cuenta de usuario está disponible en la pestaña **Usuarios** de la sección **Usuarios y funciones** → **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 funciones** → **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 de configuración que se abre, 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 está activada la opción **Mostrar la consola en modo de solo panel**, pulse el botón de alternancia para desactivarla.

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** está disponible para el usuario de 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 **Control e informes** → **Panel**. Podrá hacer lo siguiente:

- [Agregar nuevos widgets](#) al panel.
- [Ocultar widgets](#) que el usuario no necesita.

- [Mover widgets](#) para ponerlos en un orden específico.
- [Cambiar el tamaño o la apariencia](#) de los widgets.
- [Cambiar la configuración de los widgets](#).

6. Pulse el botón de alternancia para activar la opción **Mostrar la consola en modo de 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 mantiene la opción desactivada, se muestra el menú principal para el usuario, de modo que pueda realizar varias acciones en Kaspersky Security Center Linux, entre ellas cambiar la configuración de seguridad y los widgets.

7. Haga clic en el botón **Guardar** cuando termine 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 compatibles de Kaspersky y necesita derechos de acceso para hacerlo, [configure los derechos](#) del usuario. Tras ello, el usuario verá los datos de las aplicaciones de Kaspersky en los widgets correspondientes a esas aplicaciones.

Ahora el usuario puede iniciar sesión en Kaspersky Security Center Linux con la cuenta personalizada y monitorear las estadísticas de protección de la red en el modo Solo panel.

## 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 **Control e informes** y haga clic en **Informes**.

Por defecto, los informes contienen información de los últimos treinta días.

Kaspersky Security Center Linux tiene un conjunto predeterminado de informes de las siguientes categorías:

- **Estado de la protección**
- **Despliegue**
- **Actualización**
- **Estadísticas de amenazas**
- **Otro**

Puede [crear plantillas de informe personalizadas](#) y [modificar](#) o [eliminar](#) las plantillas de informe existentes.

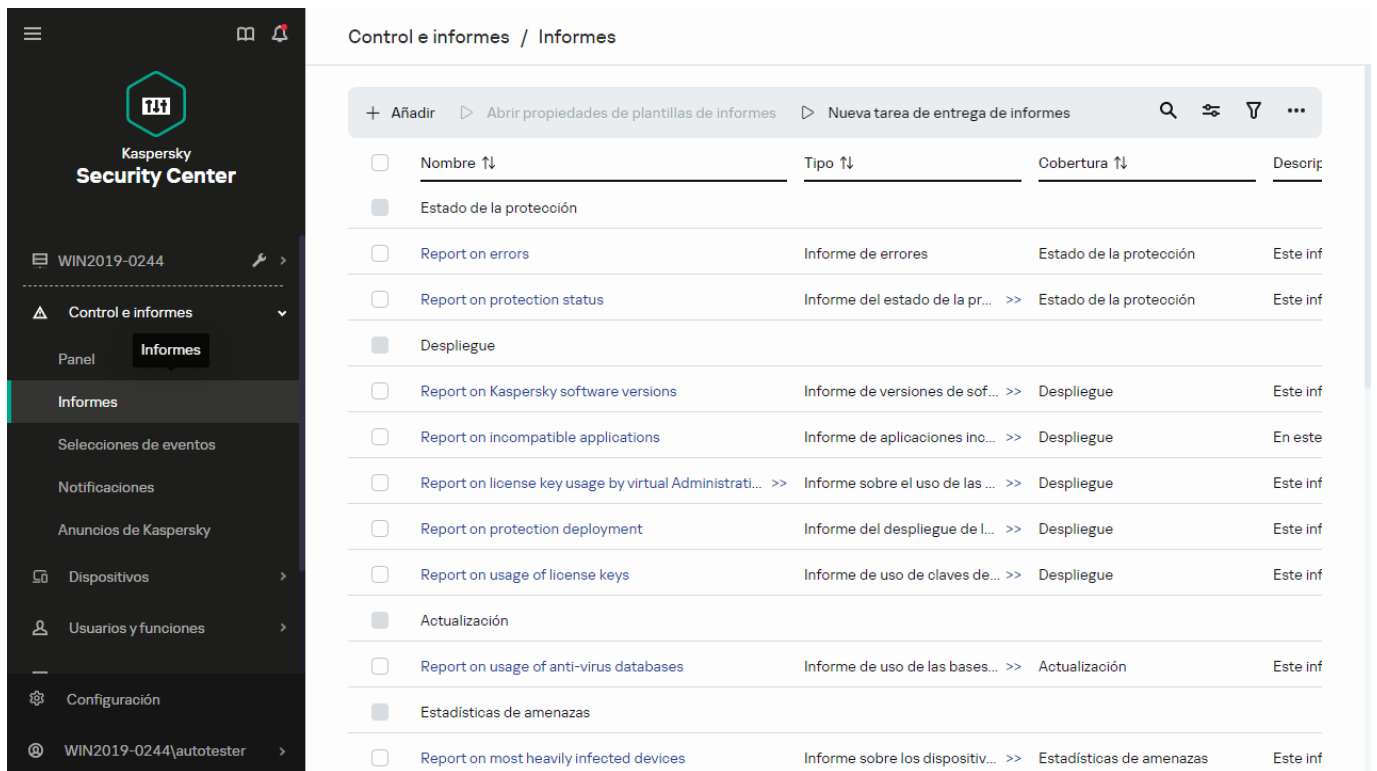


Puede [crear informes](#) que se basan en plantillas existentes, [exportar informes a archivos](#) y [crear tareas para la entrega del informe](#).

## Crear una plantilla de informe

Para crear una plantilla de informe:

1. En el menú principal, vaya a **Control e informes** → **Informes**.



Control e informes / Informes

+ Añadir ▷ Abrir propiedades de plantillas de informes ▷ Nueva tarea de entrega de informes 🔍 ⚙️ 🗑️ ...

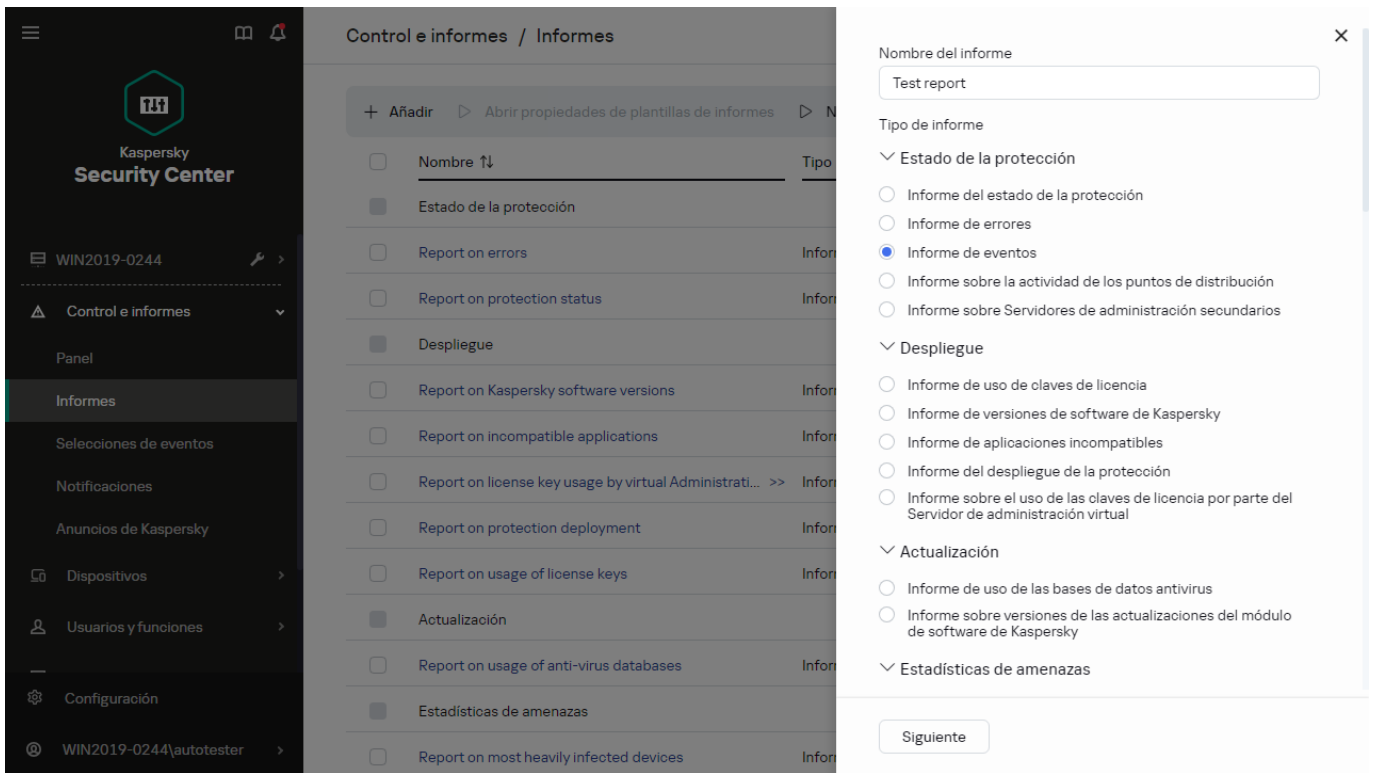
| <input type="checkbox"/> | Nombre ↕                                                  | Tipo ↕                             | Cobertura ↕              | Descripción |
|--------------------------|-----------------------------------------------------------|------------------------------------|--------------------------|-------------|
| <input type="checkbox"/> | Estado de la protección                                   |                                    |                          |             |
| <input type="checkbox"/> | Report on errors                                          | Informe de errores                 | Estado de la protección  | Este inf    |
| <input type="checkbox"/> | Report on protection status                               | Informe del estado de la pr... >>  | Estado de la protección  | Este inf    |
| <input type="checkbox"/> | Despliegue                                                |                                    |                          |             |
| <input type="checkbox"/> | Report on Kaspersky software versions                     | Informe de versiones de sof... >>  | Despliegue               | Este inf    |
| <input type="checkbox"/> | Report on incompatible applications                       | Informe de aplicaciones inc... >>  | Despliegue               | En este     |
| <input type="checkbox"/> | Report on license key usage by virtual Administrati... >> | Informe sobre el uso de las ... >> | Despliegue               | Este inf    |
| <input type="checkbox"/> | Report on protection deployment                           | Informe del despliegue de l... >>  | Despliegue               | Este inf    |
| <input type="checkbox"/> | Report on usage of license keys                           | Informe de uso de claves de... >>  | Despliegue               | Este inf    |
| <input type="checkbox"/> | Actualización                                             |                                    |                          |             |
| <input type="checkbox"/> | Report on usage of anti-virus databases                   | Informe de uso de las bases... >>  | Actualización            | Este inf    |
| <input type="checkbox"/> | Estadísticas de amenazas                                  |                                    |                          |             |
| <input type="checkbox"/> | Report on most heavily infected devices                   | Informe sobre los dispositiv... >> | Estadísticas de amenazas | Este inf    |

La lista de plantillas de informes en la subsección Informes

2. Haga clic en **Añadir**.

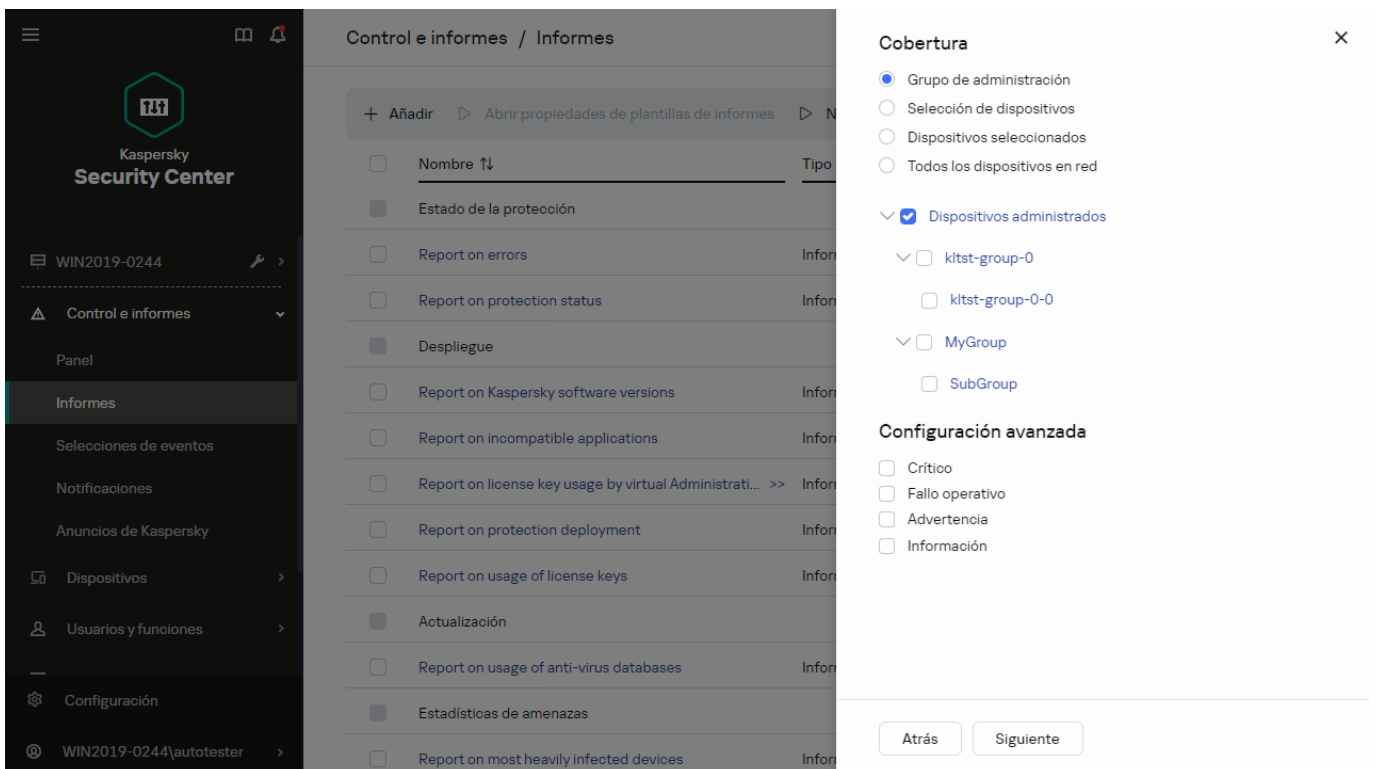
Se inicia el Asistente de nueva plantilla de informe. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En la primera página del asistente, introduzca el nombre del informe y seleccione el tipo de informe.



El Asistente de nueva plantilla de informe. Especificación del nombre y tipo de plantilla de informe

4. En la página del asistente **Cobertura**, 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.



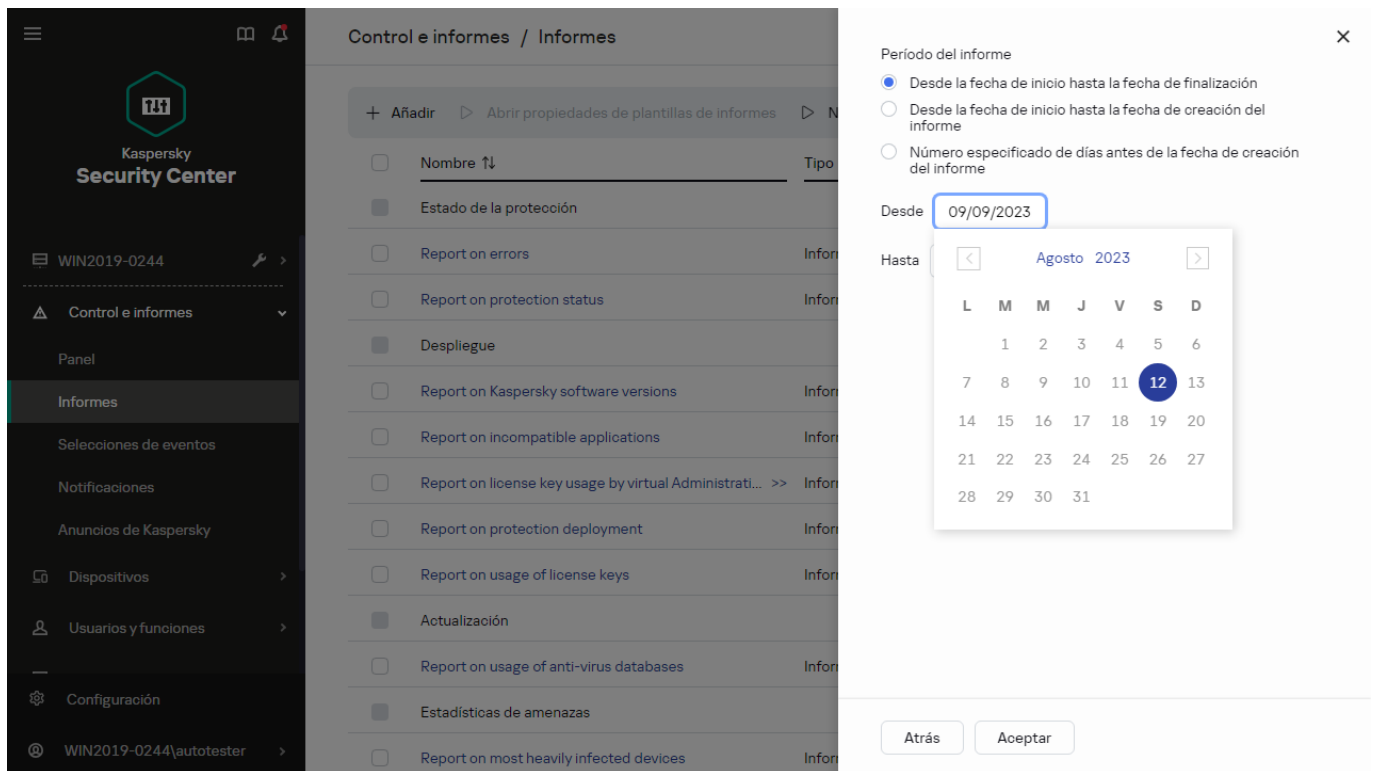
El Asistente de nueva plantilla de informe. Especificación del alcance de la plantilla de informe

5. En la página del asistente **Período del informe**, especifique el periodo 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.



El Asistente de nueva plantilla de informe. Especificación del período del informe

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 **Control 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 propiedades de plantillas de informes**.

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
- **Número máximo de entradas que mostrar** 

Si esta opción está habilitada, la tabla con los datos detallados del informe mostrará, como máximo, el número de entradas indicado aquí. Tenga en cuenta que esta opción no afecta el número máximo de eventos que puede incluir en el informe cuando [exporta el informe a un archivo](#).

Las entradas del informe se ordenan primero siguiendo las reglas especificadas en la sección **Campos** → **Campos detallados** 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 habilitada de manera 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 habilitada de manera 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 **Copiar en caché datos de los Servidores de administración secundarios** está habilitada, mostrará información tomada de la caché.

El valor predeterminado es 5 (minutos).

- [Copiar en caché 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 manera 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 manera predeterminada.

- Pestaña **Campos**

Seleccione los campos que se mostrarán en el informe y ordénelos con los botones **Subir** y **Bajar**. Use los botones **Añadir** o **Editar** para especificar si los campos se usarán para filtrar y ordenar los datos del informe.

La sección **Filtros de los campos de 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 detallados** 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 guardar uno o varios informes como XML, HTML o PDF. Kaspersky Security Center Linux le permite exportar al mismo tiempo hasta 10 informes a archivos del formato especificado.

*Para exportar un informe a un archivo:*

1. En el menú principal, vaya a **Control e informes** → **Informes**.

2. Elija los informes que desea exportar.

Si selecciona más de 10 informes, el botón **Exportar informe** estará desactivado.

3. Haga clic en el botón **Exportar informe**.

4. En la ventana que se abre, defina los siguientes parámetros de exportación:

- **Nombre del archivo.**

Si selecciona un informe para la exportación, especifique el nombre del archivo del informe.

Si selecciona más de un informe, los nombres de archivo del informe coincidirán con el nombre de las plantillas de informe seleccionadas.

- **Número máximo de entradas.**

Especifique el número máximo de entradas que se incluirán en el archivo de informe. El valor predeterminado es 10000.

Puede exportar un informe con un número ilimitado de entradas. Tenga en cuenta que si su informe contiene una gran cantidad de entradas, aumenta el tiempo necesario para generarlo y exportarlo.

- **Formato de archivo.**

Seleccione el formato de archivo del informe: XML, HTML o PDF. Si exporta varios informes, todos los informes seleccionados se guardan en el formato especificado como archivos independientes.

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.

5. Haga clic en el botón **Exportar informe**.

El informe se guarda en un archivo en el formato especificado.

## Generación y visualización de un informe

*Para crear y ver un informe:*

1. En el menú principal, vaya a **Control 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.

En los informes generados, algunas fuentes pueden mostrarse incorrectamente en los diagramas. Para resolver este problema, instale la biblioteca fontconfig. Además, verifique que las fuentes correspondientes a la configuración regional de su sistema operativo estén instaladas en el sistema operativo.

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 **Control e informes** → **Informes**.
2. [Opcional] Marque 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 **Nueva tarea de entrega de informes**.
4. Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
5. En la primera página del asistente, introduzca el nombre de la tarea. El nombre predeterminado es **Entregar informes (<N>)**, donde <N> es el número secuencial de la tarea.
6. En la página de configuración de tareas del asistente, especifique la siguiente configuración:
  - a. Seleccione las plantillas de informe que entregará la tarea. Si seleccionó estas plantillas en el paso 2, omita este punto.
  - 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.
  - 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).
7. Si desea modificar otros valores de la tarea después de crear la tarea, en la página **Finalizar la creación de tareas** del asistente, active la opción **Abrir los detalles de la tarea cuando se complete la creación**.
8. Haga clic en el botón **Crear** para crear la tarea y cerrar el asistente.

Se creará la tarea de entrega de informes. Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, 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 **Control 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

Esta sección proporciona información sobre eventos y selecciones de eventos, sobre los tipos de eventos que ocurren en los componentes de Kaspersky Security Center Linux y sobre cómo administrar el bloqueo de eventos frecuentes.

## Acerca de los eventos en Kaspersky Security Center Linux

Kaspersky Security Center Linux 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.

### Eventos por tipo

En Kaspersky Security Center Linux 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.

### Eventos por origen

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.

Los eventos pueden ser generados por las siguientes aplicaciones:

- Componentes de Kaspersky Security Center Linux:
  - [Servidor de administración](#)
  - [Agente de red](#)
- Aplicaciones administradas por Kaspersky  
Para obtener detalles sobre los eventos generados por las aplicaciones administradas por Kaspersky, consulte la documentación de la aplicación correspondiente.

### Eventos por nivel de importancia

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 puede verlo o modificarlo en Kaspersky Security Center Linux. 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.

## Eventos de los componentes de Kaspersky Security Center Linux

Cada componente de Kaspersky Security Center Linux tiene su propio conjunto de tipos de evento. Esta sección enumera los tipos de eventos que ocurren en el Servidor de administración y el Agente de red de Kaspersky Security Center. 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 Linux 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 Linux 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 de los eventos: [Establecer el plazo de almacenamiento para un evento](#)

## 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

La siguiente tabla muestra los 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.

Eventos del Servidor de administración: nivel Crítico

| 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 licencias        | 4099                   | KLSRV_EV_LICENSE_CHECK_MORE_110 | <p>Una vez al día, Kaspersky Security Center Linux comprueba si se ha excedido alguna restricción de licencia.</p> <p>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 <a href="#">unidades con licencia</a> cubiertas por una sola licencia.</p> | 180 días                               |

|                                              |      |                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |          |
|----------------------------------------------|------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|                                              |      |                        | <p>Los dispositivos cliente se mantienen protegidos aun cuando ocurre este evento.</p> <p>Puede responder al evento de los siguientes modos:</p> <ul style="list-style-type: none"> <li>• Revise la lista de dispositivos administrados. Elimine los dispositivos que no estén en uso.</li> <li>• Agregue una licencia para más dispositivos (agregue un código de activación válido o un archivo de clave en el Servidor de administración).</li> </ul> <p>Kaspersky Security Center Linux determina las <a href="#">reglas para generar eventos</a> cuando se excede una restricción de licencia.</p> |          |
| Se ha perdido la conexión con el dispositivo | 4111 | KLSRV_HOST_OUT_CONTROL | <p>Este tipo de evento ocurre cuando un dispositivo administrado es visible en la red, pero no se ha conectado en un período específico al Servidor de administración.</p> <p>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.</p>                                                                                                                                                                                       | 180 días |

|                                                                       |             |                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                 |
|-----------------------------------------------------------------------|-------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <p><b>El estado del dispositivo es Crítico</b></p>                    | <p>4113</p> | <p>KLSRV_HOST_STATUS_CRITICAL</p>       | <p>Este tipo de evento ocurre cuando se le asigna el estado <i>Crítico</i> a un dispositivo administrado. Puede <a href="#">configurar las condiciones</a> bajo las cuales el estado del dispositivo se cambia a <i>Crítico</i>.</p>                                                                                                                                                                                                                                                                                                                                                  | <p>180 días</p> |
| <p><b>El archivo clave se ha añadido a la lista de rechazados</b></p> | <p>4124</p> | <p>KLSRV_LICENSE_BLACKLISTED</p>        | <p>Este tipo de evento ocurre cuando Kaspersky ha agregado el código de activación o el archivo de clave utilizados a la lista de rechazados.</p> <p>Comuníquese con nuestro servicio de soporte técnico para más información.</p>                                                                                                                                                                                                                                                                                                                                                    | <p>180 días</p> |
| <p><b>La licencia caduca pronto</b></p>                               | <p>4129</p> | <p>KLSRV_EV_LICENSE_SRV_EXPIRE_SOON</p> | <p>Este tipo de evento ocurre cuando se acerca la fecha de caducidad de una <a href="#">licencia comercial</a>.</p> <p>Una vez al día, Kaspersky Security Center Linux comprueba si se acerca la fecha de caducidad de la licencia. 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. Este número de días no se puede cambiar. 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.</p> | <p>180 días</p> |

|                                   |      |                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |          |
|-----------------------------------|------|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|                                   |      |                           | <p>Cuando caduca la licencia comercial, Kaspersky Security Center Linux presta solo la <a href="#">funcionalidad básica</a>.</p> <p>Puede responder al evento de los siguientes modos:</p> <ul style="list-style-type: none"> <li>• Asegúrese de tener una <a href="#">clave de licencia de reserva</a> agregada en el Servidor de administración.</li> <li>• Si usa una <a href="#">suscripción</a>, no olvide renovarla. Una suscripción ilimitada se renueva automáticamente si el proveedor de servicios recibe a término y por adelantado el pago correspondiente.</li> </ul> |          |
| <b>El certificado ha caducado</b> | 4132 | KLSRV_CERTIFICATE_EXPIRED | <p>Este tipo de evento ocurre cuando caduca el certificado del Servidor de administración para Administración de dispositivos móviles.</p> <p>Deberá actualizar el certificado caducado.</p> <p>Puede configurar actualizaciones automáticas de certificados seleccionando la casilla de verificación <b>Reemitir el certificado automáticamente siempre que sea posible</b> en la configuración de emisión del certificado.</p>                                                                                                                                                   | 180 días |

## Eventos del Servidor de administración: nivel Error funcional

La siguiente tabla muestra los eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Fallo operativo**.

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 |
|------------------------------------------------------------------------------------------------------|------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| <b>Error en tiempo de ejecución</b>                                                                  | 4125                   | KLSRV_RUNTIME_ERROR      | <p>Los eventos de este tipo ocurren debido a problemas desconocidos.</p> <p>En la mayoría de los casos, estos son problemas de DBMS, problemas de red y otros problemas de software y hardware.</p> <p>Los detalles del evento se pueden encontrar en la descripción del evento.</p>                                                                                                                                                                                                                                                       | 180 días                               |
| <b>Se ha superado el límite de instalaciones para uno de los grupos de aplicaciones con licencia</b> | 4126                   | KLSRV_INVLICPROD_EXCEDED | <p>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 Linux y si el número de instalaciones ha superado el límite establecido por la clave de licencia de la aplicación de terceros.</p> <p>Puede responder al evento de los siguientes modos:</p> <ul style="list-style-type: none"><li>• Revise la lista de dispositivos administrados. Si la aplicación del</li></ul> | 180 días                               |

|                                                                       |      |                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |          |
|-----------------------------------------------------------------------|------|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|                                                                       |      |                     | <p>tercero no se está utilizando en algún dispositivo, desinstálela de ese equipo.</p> <ul style="list-style-type: none"> <li>• Solicite al tercero una licencia para más dispositivos.</li> </ul> <p>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.</p>                                                                                                                                            |          |
| <b>Error al copiar las actualizaciones en la carpeta especificada</b> | 4123 | KLSRV_UPD_REPL_FAIL | <p>Los eventos de este tipo se producen cuando las actualizaciones de software se copian en una carpeta compartida adicional.</p> <p>Puede responder al evento de los siguientes modos:</p> <ul style="list-style-type: none"> <li>• Verifique si la cuenta de usuario que se emplea para obtener acceso a la(s) carpeta(s) tiene permiso de escritura.</li> <li>• Compruebe si cambió un nombre de usuario y / o una contraseña de la carpeta(s).</li> <li>• 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.</li> </ul> | 180 días |



|                                                                                                 |             |                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                 |
|-------------------------------------------------------------------------------------------------|-------------|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <p><b>No queda espacio libre en el disco</b></p>                                                | <p>4107</p> | <p>KLSRV_DISK_FULL</p>                 | <p>Los eventos de este tipo ocurren cuando el disco duro del dispositivo donde está instalado el Servidor de administración se queda sin espacio libre.</p> <p>Libere espacio en el disco del dispositivo.</p>                                                                                                                                                                                                                                                                                                         | <p>180 días</p> |
| <p><b>La carpeta compartida no está disponible</b></p>                                          | <p>4108</p> | <p>KLSRV_SHARED_FOLDER_UNAVAILABLE</p> | <p>Los eventos de este tipo se producen si la <a href="#">carpeta compartida del Servidor de administración</a> no está disponible.</p> <p>Puede responder al evento de los siguientes modos:</p> <ul style="list-style-type: none"> <li>• Compruebe si el Servidor de administración (donde se encuentra la carpeta compartida) está encendido y disponible.</li> <li>• Compruebe si se cambió/cambiaron un nombre de usuario y / o una contraseña de la carpeta.</li> <li>• Compruebe la conexión de red.</li> </ul> | <p>180 días</p> |
| <p><b>La base de datos de información del Servidor de administración no está disponible</b></p> | <p>4109</p> | <p>KLSRV_DATABASE_UNAVAILABLE</p>      | <p>Los eventos de este tipo ocurren si la base de datos del Servidor de administración deja de estar disponible.</p> <p>Puede responder al evento de los siguientes modos:</p> <ul style="list-style-type: none"> <li>• Compruebe si el servidor remoto que tiene instalado SQL Server está disponible.</li> <li>• Vea los registros de DBMS para descubrir el motivo</li> </ul>                                                                                                                                       | <p>180 días</p> |

|                                                                                |      |                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |          |
|--------------------------------------------------------------------------------|------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|                                                                                |      |                     | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |          |
| <b>No hay espacio libre en la base de datos del Servidor de administración</b> | 4110 | KLSRV_DATABASE_FULL | <p>Los eventos de este tipo ocurren cuando no hay espacio libre en la base de datos del Servidor de administración.</p> <p>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.</p> <p>Las siguientes son las causas de este evento (agrupadas por DBMS) y distintas maneras en las que puede responder al mismo:</p> <ul style="list-style-type: none"> <li>• Si su DBMS es SQL Server Express Edition: <ul style="list-style-type: none"> <li>• 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.</li> </ul> </li> </ul> | 180 días |

- [Limite el número de eventos que se almacenan en la base de datos del Servidor de administración.](#)

- En la base de datos del Servidor de administración hay demasiados eventos enviados por el componente Control de aplicaciones. Puede cambiar la configuración de la directiva de Kaspersky Endpoint Security relacionada con el almacenamiento de eventos del Control de aplicaciones en la base de datos del Servidor de administración.

- Si su DBMS no es SQL Server Express Edition:

- [No limite el número de eventos para almacenar en la base de datos del Servidor de administración.](#)

- [Reduzca la lista de eventos para almacenar en la base de datos del Servidor de administración.](#)

Revise la información sobre la [selección del DBMS.](#)

## 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 ha detectado 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: <a href="#">Bloquear eventos frecuentes</a> .                                                                                                                                                                                                          | 90 días                                |
| Se ha superado el límite de licencias        | 4098                   | KLSRV_EV_LICENSE_CHECK_100_110   | Una vez al día, Kaspersky Security Center Linux comprueba si se ha excedido alguna restricción de licencia.<br><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 <a href="#">unidades con licencia</a> cubiertas por una sola licencia. | 90 días                                |

|                                                                                     |      |                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |         |
|-------------------------------------------------------------------------------------|------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                                                                     |      |                               | <p>Los dispositivos cliente se mantienen protegidos aun cuando ocurre este evento.</p> <p>Puede responder al evento de los siguientes modos:</p> <ul style="list-style-type: none"> <li>• Revise la lista de dispositivos administrados. Elimine los dispositivos que no estén en uso.</li> <li>• Agregue una licencia para más dispositivos (agregue un código de activación válido o un archivo de clave en el Servidor de administración).</li> </ul> <p>Kaspersky Security Center Linux determina las <a href="#">reglas para generar eventos</a> cuando se excede una restricción de licencia.</p> |         |
| <p><b>El dispositivo ha permanecido inactivo en la red durante mucho tiempo</b></p> | 4103 | KLSRV_EVENT_HOSTS_NOT_VISIBLE | <p>Este tipo de evento ocurre cuando un dispositivo administrado se encuentra inactivo durante cierto tiempo.</p> <p>La mayoría de las veces, esto sucede porque el dispositivo se ha dado de baja.</p> <p>Puede responder al evento de los siguientes modos:</p> <ul style="list-style-type: none"> <li>• Elimine el dispositivo manualmente de la lista de dispositivos administrados.</li> </ul>                                                                                                                                                                                                     | 90 días |

|                                            |      |                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |
|--------------------------------------------|------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                            |      |                            | <p>Especifique el intervalo de tiempo después del cual se crea el evento <b>El dispositivo ha permanecido inactivo en la red durante mucho tiempo</b> mediante <a href="#">Kaspersky Security Center Web Console</a>.</p> <ul style="list-style-type: none"> <li>Especifique el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo mediante <a href="#">Kaspersky Security Center Web Console</a>.</li> </ul>                                                                                                                                            |         |
| <b>Conflicto de nombres de dispositivo</b> | 4102 | KLSRV_EVENT_HOSTS_CONFLICT | <p>Este tipo de evento ocurre cuando el Servidor de administración considera que dos o más dispositivos administrados son un mismo dispositivo.</p> <p>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.</p> <p>Para evitar este problema, ponga el Agente de red en <a href="#">modo de clonación de disco</a> en el dispositivo de referencia antes de clonar el disco duro de ese dispositivo.</p> | 90 días |

|                                                                                                               |             |                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                |
|---------------------------------------------------------------------------------------------------------------|-------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <p><b>El estado del dispositivo es Advertencia</b></p>                                                        | <p>4114</p> | <p>KLSRV_HOST_STATUS_WARNING</p> | <p>Este tipo de evento ocurre cuando se le asigna el estado <i>Advertencia</i> a un dispositivo administrado. Puede <a href="#">configurar las condiciones</a> en las cuales el estado del dispositivo se cambia a <i>Advertencia</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <p>90 días</p> |
| <p><b>Pronto se superará el límite de instalaciones de uno de los grupos de aplicaciones con licencia</b></p> | <p>4127</p> | <p>KLSRV_INVLICPROD_FILLED</p>   | <p>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.</p> <p>Puede responder al evento de los siguientes modos:</p> <ul style="list-style-type: none"> <li>• Si la aplicación de terceros no se utiliza en algunos de los dispositivos administrados, elimínela de esos dispositivos.</li> <li>• 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.</li> </ul> | <p>90 días</p> |

|                                 |      |                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |         |
|---------------------------------|------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                 |      |                             | Para administrar las claves de licencia de sus aplicaciones de terceros, puede utilizar la característica de grupos de aplicaciones con licencia.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |         |
| Se ha solicitado el certificado | 4133 | KLSRV_CERTIFICATE_REQUESTED | <p>Este tipo de evento ocurre cuando un certificado de la característica Administración de dispositivos móviles no se vuelve a emitir automáticamente.</p> <p>Estas pueden ser las causas del evento y las respuestas adecuadas:</p> <ul style="list-style-type: none"> <li>• Se ha iniciado la nueva emisión automática de un certificado para el que la opción <b>Reemitir el certificado automáticamente siempre que sea posible</b> está desactivada. Esto puede deberse a un error ocurrido durante la creación del certificado. Es posible que se requiera la reemisión manual del certificado.</li> <li>• 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</li> </ul> | 90 días |



|                                               |      |                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                |
|-----------------------------------------------|------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
|                                               |      |                                    | las propiedades de la cuenta.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                |
| <b>El certificado se ha eliminado</b>         | 4134 | KLSRV_CERTIFICATE_REMOVED          | <p>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.</p> <p>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.</p> <p>Este evento puede resultar útil a la hora de investigar fallas asociadas con la administración de dispositivos móviles.</p> | 90 días        |
| <b>El certificado de APNs ha caducado</b>     | 4135 | KLSRV_APN_CERTIFICATE_EXPIRED      | <p>Este tipo de evento ocurre cuando caduca un certificado de APNs.</p> <p>Debe renovar manualmente el certificado de APNs e instalarlo en un servidor de MDM para iOS.</p>                                                                                                                                                                                                                                                                                                                                   | No se almacena |
| <b>El certificado de APNs caducará pronto</b> | 4136 | KLSRV_APN_CERTIFICATE_EXPIRES_SOON | <p>Este tipo de evento ocurre cuando quedan menos de catorce días para que caduque el certificado de APNs.</p> <p>Cuando el certificado de APNs caduque, deberá renovarlo manualmente e instalarlo en un servidor de MDM para iOS.</p>                                                                                                                                                                                                                                                                        | No se almacena |

|                                                                             |      |                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |         |
|-----------------------------------------------------------------------------|------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                                                             |      |                        | Le recomendamos que programe la renovación del certificado de APNs para antes de la fecha de caducidad.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |         |
| <b>No se ha podido enviar el mensaje FCM al dispositivo móvil</b>           | 4138 | KLSRV_GCM_DEVICE_ERROR | <p>Este tipo de evento ocurre cuando la característica Administración de dispositivos móviles se ha configurado para que la conexión a los dispositivos Android administrados se establezca utilizando Google Firebase Cloud Messaging (FCM) y el servidor de FCM no puede atender algunas de las solicitudes enviadas por el Servidor de administración. Lo que esto significa es que algunos de los dispositivos móviles administrados no recibirán una notificación push.</p> <p>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 <a href="#">documentación del servicio Google Firebase</a> (en especial, el capítulo “Códigos de respuesta de errores de mensajes descendentes”).</p> | 90 días |
| <b>Se produjo un error de HTTP al enviar el mensaje FCM al servidor FCM</b> | 4139 | KLSRV_GCM_HTTP_ERROR   | Este tipo de evento ocurre cuando la característica Administración de dispositivos móviles está configurada para utilizar Google                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 90 días |

|                                                                       |             |                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                |
|-----------------------------------------------------------------------|-------------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
|                                                                       |             |                                | <p>           Firebase Cloud Messaging (FCM) para la conexión de dispositivos móviles Android administrados y el servidor de FCM responde a una solicitud del Servidor de administración con un código HTTP distinto de 200 (OK).         </p> <p>           Estas pueden ser las causas del evento y las respuestas adecuadas:         </p> <ul style="list-style-type: none"> <li>           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 <a href="#">documentación del servicio Google Firebase</a> (en especial, el capítulo "Códigos de respuesta de errores de mensajes descendentes").         </li> <li>           Problemas en el servidor proxy (si usa un servidor proxy). Lea el código HTTP en los detalles del evento y actúe en consecuencia.         </li> </ul> |                |
| <p> <b>No se ha podido enviar el mensaje FCM al servidor FCM</b> </p> | <p>4140</p> | <p>KLSRV_GCM_GENERAL_ERROR</p> | <p>           Este tipo de evento ocurre cuando suceden errores inesperados del lado del Servidor de administración al         </p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p>90 días</p> |

|                                                                              |      |                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |         |
|------------------------------------------------------------------------------|------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                                                              |      |                            | <p>utilizar el protocolo HTTP de Google Firebase Cloud Messaging.</p> <p>Lea los detalles en la descripción del evento y responda en consecuencia.</p> <p>Si no puede encontrar la solución a un problema por su cuenta, le recomendamos que se comuniquen con el servicio de soporte técnico de Kaspersky.</p>                                                                                                                                                                                                                                                                                    |         |
| <b>Poco espacio libre en el disco duro</b>                                   | 4105 | KLSRV_NO_SPACE_ON_VOLUMES  | <p>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.</p> <p>Libere espacio en el disco del dispositivo.</p>                                                                                                                                                                                                                                                                                                                                                                                           | 90 días |
| <b>Poco espacio libre en la base de datos del Servidor de administración</b> | 4106 | KLSRV_NO_SPACE_IN_DATABASE | <p>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.</p> <p>Las siguientes son las causas de este evento (agrupadas por DBMS) y las distintas maneras en las que puede responder.</p> <p>Si su DBMS es SQL Server Express Edition:</p> <ul style="list-style-type: none"> <li>• En la documentación de SQL Server</li> </ul> | 90 días |

Express, revise el límite del tamaño de la base de datos de la versión que utiliza. Es probable que la base de datos del Servidor de administración esté a punto de alcanzar el tamaño máximo posible.

- [Limite el número de eventos que se almacenan en la base de datos del Servidor de administración.](#)
- 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 relacionada con el almacenamiento de eventos del Control de aplicaciones en la base de datos del Servidor de administración. Si su DBMS no es SQL Server Express Edition:
- [No limite el número de eventos que se almacenan en la base de datos del Servidor de administración.](#)
- [Reduzca la lista de eventos que se almacenan en la base de datos del](#)

|                                                                                                    |      |                                  |                                                                                                                                                                                                                                                                                                                                                       |         |
|----------------------------------------------------------------------------------------------------|------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                                                                                    |      |                                  | <p><a href="#">Servidor de administración.</a></p> <p>Revise la información sobre la <a href="#">selección del DBMS.</a></p>                                                                                                                                                                                                                          |         |
| <p><b>Se ha interrumpido la conexión con el Servidor de administración secundario</b></p>          | 4116 | KLSRV_EV_SLAVE_SRV_DISCONNECTED  | <p>Este tipo de evento ocurre cuando se interrumpe una conexión con el Servidor de administración secundario.</p> <p>Consulte el registro del sistema operativo en el dispositivo en el que esté instalado el Servidor de administración secundario y responda en consecuencia.</p>                                                                   | 90 días |
| <p><b>Se ha interrumpido la conexión con el Servidor de administración principal</b></p>           | 4118 | KLSRV_EV_MASTER_SRV_DISCONNECTED | <p>Este tipo de evento ocurre cuando se interrumpe una conexión con el Servidor de administración principal.</p> <p>Consulte el registro del sistema operativo en el dispositivo en el que esté instalado el Servidor de administración principal y responda en consecuencia.</p>                                                                     | 90 días |
| <p><b>Se han registrado las nuevas actualizaciones para los módulos del software Kaspersky</b></p> | 4141 | KLSRV_SEAMLESS_UPDATE_REGISTERED | <p>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.</p> <p>Apruebe o rechace las actualizaciones mediante Kaspersky Security Center Web Console.</p> | 90 días |

|                                                                                                                     |      |                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                |
|---------------------------------------------------------------------------------------------------------------------|------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <p>Se ha superado el límite del número de eventos en la base de datos, se ha iniciado la eliminación de eventos</p> | 4145 | KLSRV_EVP_DB_TRUNCATING | <p>Este tipo de evento ocurre cuando el sistema comienza a eliminar eventos antiguos de la base de datos del Servidor de administración <u>por haberse alcanzado el límite de capacidad de la misma.</u></p> <p>Puede responder al evento de los siguientes modos:</p> <ul style="list-style-type: none"> <li>• <u>Cambie el número de eventos que se conservará, como máximo, en la base de datos del Servidor de administración.</u></li> <li>• <u>Reduzca la lista de eventos que se almacenan en la base de datos del Servidor de administración.</u></li> </ul> | No se almacena |
| <p>Se ha superado el límite del número de eventos en la base de datos, los eventos se han eliminado</p>             | 4146 | KLSRV_EVP_DB_TRUNCATED  | <p>Este tipo de evento ocurre cuando el sistema eliminó eventos antiguos de la base de datos del Servidor de administración <u>por haberse alcanzado el límite de capacidad de la misma.</u></p> <p>Puede responder al evento de los siguientes modos:</p> <ul style="list-style-type: none"> <li>• <u>Cambie el número de eventos que se conservará, como máximo, en la base de datos del Servidor de administración.</u></li> <li>• <u>Reduzca la lista de eventos que se almacenan en la base de datos del Servidor de administración.</u></li> </ul>             | No se almacena |

## 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 ha detectado un nuevo dispositivo                                                                                          | 4100                   | KLSRV_EVENT_HOSTS_NEW_DETECTED   | 30 días                                |               |
| El dispositivo se ha añadido automáticamente al grupo                                                                         | 4101                   | KLSRV_EVENT_HOSTS_NEW_REDIRECTED | 30 días                                |               |
| El dispositivo se ha eliminado del grupo: inactivo en la red durante mucho tiempo                                             | 4104                   | KLSRV_INVISIBLE_HOSTS_REMOVED    | 30 días                                |               |
| Pronto se superará el límite de instalaciones de uno de los grupos de aplicaciones con licencia (ya se ha usado más del 95 %) | 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                                                                                                                           | 4122                   | KLSRV_UPD_REPL_OK                | 30 días                                |               |



|                                                                            |      |                               |         |                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------|------|-------------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| actualizaciones se han copiado correctamente en la carpeta especificada    |      |                               |         |                                                                                                                                                                                                                                                                                                                    |
| La conexión con el Servidor de administración secundario está establecida  | 4115 | KLSRV_EV_SLAVE_SRV_CONNECTED  | 30 días |                                                                                                                                                                                                                                                                                                                    |
| La conexión con el Servidor de administración principal está establecida   | 4117 | KLSRV_EV_MASTER_SRV_CONNECTED | 30 días |                                                                                                                                                                                                                                                                                                                    |
| Las bases de datos se han actualizado                                      | 4144 | KLSRV_UPD_BASES_UPDATED       | 30 días |                                                                                                                                                                                                                                                                                                                    |
| Auditoría: Se ha establecido la conexión con el Servidor de administración | 4147 | KLAUD_EV_SERVERCONNECT        | 30 días |                                                                                                                                                                                                                                                                                                                    |
| Auditoría: Se ha modificado el objeto                                      | 4148 | KLAUD_EV_OBJECTMODIFY         | 30 días | <p>Este evento responde a cambios ocurridos en los siguientes objetos:</p> <ul style="list-style-type: none"> <li>• Grupo de administración</li> <li>• Grupo de seguridad</li> <li>• Usuario</li> <li>• Paquete</li> <li>• Tarea</li> <li>• Directiva</li> <li>• Servidores</li> <li>• Servidor virtual</li> </ul> |
| Auditoría: El estado del objeto ha cambiado                                | 4150 | KLAUD_EV_TASK_STATE_CHANGED   | 30 días | <p>Este evento ocurre, por ejemplo, cuando una tarea no se completa debido a un error.</p>                                                                                                                                                                                                                         |

|                                                                                              |      |                             |         |                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------|------|-----------------------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Comprobar:<br>Parámetros de grupo modificados                                                | 4149 | KLAUD_EV_ADMGROUP_CHANGED   | 30 días |                                                                                                                                                                                                           |
| Auditoría: Se ha finalizado la conexión al Servidor de administración                        | 4151 | KLAUD_EV_SERVERDISCONNECT   | 30 días |                                                                                                                                                                                                           |
| Auditoría: Se han modificado las propiedades del objeto                                      | 4152 | KLAUD_EV_OBJECTPROPMODIFIED | 30 días | Este evento responde a cambios ocurridos en las siguientes propiedades: <ul style="list-style-type: none"> <li>• Usuario</li> <li>• Licencia</li> <li>• Servidores</li> <li>• Servidor virtual</li> </ul> |
| Auditoría: Se han modificado los permisos de usuario                                         | 4153 | KLAUD_EV_OBJECTACLMODIFIED  | 30 días |                                                                                                                                                                                                           |
| Auditoría: las claves de cifrado se han importado o exportado del Servidor de administración | 5100 | KLAUD_EV_DPEKEYSEXPORT      | 30 días |                                                                                                                                                                                                           |

## 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 Advertencia

La siguiente tabla muestra los eventos del Agente de red 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 | Id. del | Tipo de evento | Plazo de |
|-------------------------------|---------|----------------|----------|
|-------------------------------|---------|----------------|----------|

| tipo de evento                                                                       | tipo de evento |                                 | almacenamiento predeterminado |
|--------------------------------------------------------------------------------------|----------------|---------------------------------|-------------------------------|
| Ocurrió un problema de seguridad                                                     | 549            | GNRL_EV_APP_INCIDENT_OCCURED    | 30 días                       |
| Se ha iniciado el proxy de KSN. Error en la comprobación de la disponibilidad de KSN | 7718           | KSNPROXY_STARTED_CON_CHK_FAILED | 30 días                       |

## Eventos del Agente de red: nivel Información

La siguiente tabla muestra los eventos del Agente de red 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 aplicación se ha instalado                                                                           | 7703                   | KLNAG_EV_INV_APP_INSTALLED       | 30 días                                |
| La aplicación se ha desinstalado                                                                        | 7704                   | KLNAG_EV_INV_APP_UNINSTALLED     | 30 días                                |
| La aplicación supervisada se ha instalado                                                               | 7705                   | KLNAG_EV_INV_OBS_APP_INSTALLED   | 30 días                                |
| La aplicación supervisada se ha desinstalado                                                            | 7706                   | KLNAG_EV_INV_OBS_APP_UNINSTALLED | 30 días                                |
| Se ha añadido un nuevo dispositivo                                                                      | 7708                   | KLNAG_EV_DEVICE_ARRIVAL          | 30 días                                |
| El dispositivo se ha eliminado                                                                          | 7709                   | KLNAG_EV_DEVICE_REMOVE           | 30 días                                |
| Se ha detectado un nuevo dispositivo                                                                    | 7710                   | KLNAG_EV_NAC_DEVICE_DISCOVERED   | 30 días                                |
| El dispositivo se ha autorizado                                                                         | 7711                   | KLNAG_EV_NAC_HOST_AUTHORIZED     | 30 días                                |
| El proxy de KSN se ha iniciado. La comprobación de disponibilidad de KSN se ha completado correctamente | 7719                   | KSNPROXY_STARTED_CON_CHK_OK      | 30 días                                |
| El proxy de KSN se ha detenido                                                                          | 7720                   | KSNPROXY_STOPPED                 | 30 días                                |

## 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**, **Fallos operativos**, **Advertencias** y **Eventos de información**
- Por fecha: **Eventos recientes**
- Por tipo: **Solicitudes de los usuarios** 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 **Control 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 Linux tiene un conjunto predeterminado de las selecciones (predefinidas) del evento:

- Eventos con distintos niveles de importancia:
  - **Eventos críticos**
  - **Errores funcionales**
  - **Advertencias**
  - **Mensajes de información**
- **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 Linux 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 **Control e informes** → **Selecciones de eventos**.
2. Haga clic en **Añadir**.
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 **Control 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 **Control 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 y comenzar**.
    - 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 Linux le permite guardar una selección de eventos y su configuración en un archivo KLO. Puede utilizar este archivo KLO para [importar la selección de eventos guardada](#) tanto a Kaspersky Security Center Windows como a 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 Linux (selecciones predefinidas) no se pueden guardar en un archivo.

*Para exportar una selección de eventos:*

1. En el menú principal, vaya a **Control e informes** → **Selecciones de eventos**.
2. Marque la casilla junto a la selección de eventos que desea exportar.

No puede exportar varias selecciones de eventos al mismo tiempo. Si selecciona más de una selección, el botón **Exportar** se desactivará.
3. Haga clic en el botón **Exportar**.
4. En la ventana **Guardar como** que se abre, especifique el nombre y la ruta del archivo de selección de eventos y, a continuación, haga clic en el botón **Guardar**.

La ventana **Guardar como** se muestra solo si usa Google Chrome, Microsoft Edge u Opera. Si utiliza otro navegador, el archivo de selección de eventos se guarda automáticamente en la carpeta **Descargas**.

## Importar una selección de eventos

Kaspersky Security Center Linux le permite importar una selección de eventos desde un archivo KLO. El archivo KLO contiene la [selección de eventos exportados](#) y su configuración.

*Para importar una selección de eventos:*

1. En el menú principal, vaya a **Control e informes** → **Selecciones de eventos**.
2. Haga clic en el botón **Importar** y elija un archivo de selección de eventos que desee importar.
3. En la ventana abierta, especifique la ruta al archivo KLO y luego haga clic en el botón **Abrir**. Tenga en cuenta que solo puede seleccionar un archivo de selección de eventos.  
Se inicia el procesamiento de selección de eventos.

Aparece la notificación con los resultados de la importación. Si la selección de eventos se importa correctamente, puede hacer clic en el enlace **Ver detalles de importación** para ver las propiedades de la selección de eventos.

Después de una importación correcta, la selección de eventos se muestra en la lista de selecciones. La configuración de la selección de eventos también se importa.

Si la selección de eventos recién importada tiene un nombre idéntico al de una selección de eventos existente, al nombre de la selección importada se le añade un índice (**<número de secuencia siguiente>**), 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

*Para exportar eventos a un archivo:*

1. [Genere una selección de eventos.](#)

2. Active la casilla de verificación ubicada junto al evento pertinente.

3. Haga clic en el botón **Exportar a archivo**.

El evento seleccionado se exporta a un archivo.

## 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. Active la casilla de verificación ubicada junto al evento pertinente.

3. Haga clic en el botón **Historial de revisión**.

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 **Control 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 Linux le permite recibir información sobre los eventos que ocurren durante el 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. Realice una de las siguientes acciones:

- Para configurar el plazo de almacenamiento de los eventos del Agente de red o de una aplicación de Kaspersky administrada, haga clic en el nombre de la directiva correspondiente.

Se abrirá la página de propiedades de la directiva.

- Para configurar los eventos del Servidor de administración, en el menú principal, haga clic en el icono de configuración (⚙️) al lado del nombre del Servidor de administración requerido.

Si tiene una directiva para el Servidor de administración, puede hacer clic en el nombre de esta directiva.

Se abre la página de propiedades del Servidor de administración (o la página de propiedades de la directiva del Servidor de administración).

3. Seleccione la pestaña **Configuración de eventos**.

Se muestra una lista de los tipos de evento relacionados con la sección **Crítico**.

4. Seleccione la sección **Fallo operativo**, **Advertencia** o **Información**.

5. 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 eventos** de la ventana que se abre, la opción **Almacenar en la base de datos del Servidor de administración durante (días)** está habilitada.

6. En el cuadro de edición debajo de este botón de alternancia, introduzca la cantidad de días para almacenar el evento.

7. Si no desea almacenar un evento en la base de datos del Servidor de administración, deshabilite la opción **Almacenar en la base de datos del Servidor de administración durante (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.

8. Haga clic en **Aceptar**.

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.

## 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 for Linux, 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**, seleccione la sección **Bloqueo de eventos frecuentes**.

3. En sección **Bloqueo de eventos frecuentes**:

- Si desea desbloquear la recepción de eventos frecuentes:
  - a. Seleccione los eventos frecuentes que desea desbloquear y 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 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**, seleccione la sección **Bloqueo de eventos frecuentes**.

3. En la sección **Bloqueo de eventos frecuentes**, seleccione la fila del evento frecuente cuyo bloqueo desea eliminar.

4. Haga clic en el botón **Quitar del bloqueo**.

El evento frecuente se elimina de la lista de eventos frecuentes. El Servidor de administración recibirá los eventos de este tipo.

## Almacenamiento y procesamiento de eventos en el Servidor de administración

La información sobre eventos de 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 conservar solo la cantidad máxima especificada de eventos.

Cuando el Servidor de administración elimina los eventos antiguos, no puede guardar los nuevos eventos en la base de datos. Durante este período, la información sobre los eventos que se rechazaron se escribe en el registro del sistema operativo. Los nuevos eventos se ponen en cola y se guardan en la base de datos una vez finalizada la operación de borrado.

## 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 ha realizado la acción recomendada para la notificación o ha asignado este estado para la notificación manualmente.
- *No revisado*. Significa que no ha realizado la acción recomendada para la notificación o ha asignado 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 Linux 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 **Control 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 **Control 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 **Control e informes** → **Notificaciones**.

La categoría **Todas las notificaciones** se selecciona en el panel izquierdo y en el panel derecho se muestran todas las notificaciones.

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)
- **Enlaces 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)
- **Noticias de Kaspersky** (esto incluye información sobre lanzamientos de aplicaciones 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 informativas**. 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*.
- **Estado registrado**. 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 de 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 **Añadir o restaurar un widget web**.
2. En la ventana que se abre, haga clic en la categoría **Otro**, 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 **Control e informes**.

## Acerca de los estados de los dispositivos

Kaspersky Security Center Linux 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 Linux tiene en cuenta el indicador de visibilidad del dispositivo en la red (consulte la tabla a continuación). Si Kaspersky Security Center Linux 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*
- *Correcto* o *Correcto/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.                                                                                                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• Interruptor activado.</li> <li>• Interruptor desactivado.</li> </ul> |
| Demasiados virus detectados                                                            | Una tarea de detección de virus (por ejemplo, la tarea de análisis antimalware) ha detectado algunos virus en el dispositivo y el número de virus encontrados supera el valor especificado.                                                                                                                                                                                                | Más de 0.                                                                                                     |
| El nivel de protección en tiempo real es distinto del 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.                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>• Detenida.</li> <li>• En pausa.</li> <li>• En ejecución.</li> </ul>   |
| No se ha realizado ningún análisis antimalware desde hace mucho tiempo                 | El dispositivo es visible en la red y una aplicación de seguridad está instalada en el dispositivo, pero ni la tarea <i>Análisis de malware</i> ni una tarea de análisis local se ha ejecutado durante 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.                                                                                                 |
| No conectado durante 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 <b>Amenazas activas</b> supera el valor especificado.                                                                                                                                                                                                                                                                                     | Más de 0 elementos.                                                                                           |



|                                                 |                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Se requiere reiniciar                           | 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.                                                                                          | <ul style="list-style-type: none"> <li>• Interruptor desactivado.</li> <li>• Interruptor activado.</li> </ul>                                                                                                                                                                                                                                                                                                       |
| La licencia comercial ha caducado               | El dispositivo es visible en la red, pero la licencia ha caducado.                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• Interruptor desactivado.</li> <li>• Interruptor activado.</li> </ul>                                                                                                                                                                                                                                                                                                       |
| la licencia caduca pronto                       | El dispositivo es visible en la red, pero la licencia instalada en el mismo caduca en menos días que el número de días especificado.                                                                                                                                      | Más de 0 días.                                                                                                                                                                                                                                                                                                                                                                                                      |
| 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.                                                                                                                                          | <ul style="list-style-type: none"> <li>• No cumple con la directiva porque el usuario no dio su consentimiento (solo para dispositivos externos).</li> <li>• No cumple con la directiva debido a un error.</li> <li>• Se debe reiniciar el dispositivo al aplicar la directiva.</li> <li>• No se ha especificado una directiva de cifrado.</li> <li>• No compatible.</li> <li>• Al aplicar la directiva.</li> </ul> |
| Problemas de seguridad no procesados detectados | Se han encontrado problemas de seguridad sin procesar en el dispositivo. Los problemas de seguridad pueden ser creados manualmente por el administrador o automáticamente por las aplicaciones de Kaspersky administradas que se han instalado en el dispositivo cliente. | <ul style="list-style-type: none"> <li>• Interruptor desactivado.</li> <li>• Interruptor activado.</li> </ul>                                                                                                                                                                                                                                                                                                       |

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                               |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Estado del dispositivo definido por la aplicación      | El estado del dispositivo es definido por la aplicación administrada.                                                                                                                                                                                                                                                                                                                                                       | <ul style="list-style-type: none"> <li>• Interruptor desactivado.</li> <li>• Interruptor activado.</li> </ul> |
| El dispositivo no tiene espacio disponible 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 <i>Crítico</i> o <i>Advertencia</i> cambiarán por el estado <i>Sin inconvenientes</i> 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.                                                                                                  |
| Se ha perdido la conexión con el dispositivo           | 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.                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>• Interruptor desactivado.</li> <li>• Interruptor activado.</li> </ul> |
| La protección está desactivada                         | El dispositivo es visible en la red, pero la aplicación de seguridad del dispositivo ha estado deshabilitada por un tiempo superior al especificado.<br><br>En este caso, el estado de la aplicación de seguridad es <i>detenida</i> o <i>error</i> , y difiere del siguiente: <i>iniciada</i> , <i>en ejecución</i> o <i>suspendida</i> .                                                                                  | Más de 0 minutos.                                                                                             |
| La aplicación de seguridad no se está ejecutando       | El dispositivo es visible en la red y tiene instalada una aplicación de seguridad, pero esa aplicación no se está ejecutando.                                                                                                                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>• Interruptor desactivado.</li> <li>• Interruptor activado.</li> </ul> |

Kaspersky Security Center Linux le permite configurar el cambio automático 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 especificadas. 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 Linux 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.

Quando Kaspersky Security Center Linux asigna un estado a un dispositivo, para algunas condiciones (consulte la columna Descripción de la condición) se tiene en cuenta el indicador de visibilidad. 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*.

## 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 **Se establece en Crítico si se especifican**, 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 **Se establece en Advertencia si se especifican**, 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 Linux. Según el método de la notificación elegido, están disponibles los siguientes tipos de notificaciones:

- Correo electrónico: Cuando se produce un evento, Kaspersky Security Center Linux envía una notificación a las direcciones de correo electrónico especificadas.
- SMS: Cuando se produce un evento, Kaspersky Security Center Linux 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 Linux:*

1. En el menú principal, haga clic en el ícono de configuración (🔧) ubicado junto al nombre del Servidor de administración pertinente.

La ventana de propiedades del Servidor de administración se abre 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** le permite configurar la notificación de eventos por correo electrónico.

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 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 el 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.

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.

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.

- **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.

- **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 activar la comunicación mediante 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 Linux 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 Linux 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.

Al hacer clic en el botón **Enviar mensaje de prueba**, puede verificar si ha configurado las notificaciones correctamente: la aplicación envía una notificación de prueba al destinatario que ha especificado.

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 **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 **Correo electrónico del remitente**: si este valor no está definido, se usará la dirección del destinatario. **Advertencia: Le recomendamos que no utilice una dirección de correo electrónico 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.

El campo **Mensaje de notificación** contiene el texto estándar con información sobre el evento que la aplicación envía cuando un evento ocurre. 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 enlace **Configurar límite numérico de notificaciones**, puede especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

- [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 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 el 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.

- **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.

- **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 activar la comunicación mediante 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 del 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 Linux 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 Linux no podrá conectarse al servidor SMTP.

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 **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 **Correo electrónico del remitente: si este valor no está definido, se usará la dirección del destinatario**. **Advertencia: Le recomendamos que no utilice una dirección de correo electrónico 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 **Números de teléfono de destinatarios de mensajes SMS**, especifique los números de teléfono celular de los destinatarios de la notificación 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 **Enviar mensaje de prueba** para verificar si configuró las notificaciones correctamente: la aplicación envía una notificación de prueba al destinatario que especificó.

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.

- [Archivo ejecutable para lanzar](#) 

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 enlace **Configurar límite numérico de notificaciones**, puede 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 Linux.

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 prueba

Para comprobar si se han enviado las notificaciones del evento, la aplicación utiliza la notificación de la 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. A continuación, vuelva a activar la protección en tiempo real del sistema de archivos.
2. Ejecute una tarea de análisis para los dispositivos cliente en un grupo de administración o para dispositivos específicos, incluido uno que tenga el virus EICAR.



Si la tarea de análisis se ha configurado correctamente, se detectará el virus de prueba. Si las notificaciones se configuraron correctamente, recibirá una notificación informándole que se detectó un virus.

Para abrir un registro de la prueba de detección de virus:

1. En el menú principal, vaya a **Control e informes** → **Selecciones de eventos**.
2. Haga clic en el nombre de selección **Eventos recientes**.

En la ventana que se abre, se muestra la notificación sobre el virus de prueba.

El virus de prueba EICAR no contiene código que pueda dañar su dispositivo. Sin embargo, la mayoría de fabricantes de aplicaciones de seguridad identifican este archivo como un virus. Puede descargar el virus de prueba del [sitio web oficial de EICAR](#).

## Notificaciones de eventos que se muestran al ejecutar un archivo ejecutable

Mediante la ejecución de un archivo ejecutable, Kaspersky Security Center Linux puede informar al administrador sobre los eventos que ocurran en los dispositivos cliente. El archivo ejecutable debe contener otro archivo ejecutable con marcadores del evento que se transmitirá al administrador.

Marcadores para describir un evento

| Marcador                         | Descripción del marcador                            |
|----------------------------------|-----------------------------------------------------|
| %SEVERITY%                       | Nivel de importancia del evento                     |
| %COMPUTER%                       | Nombre del dispositivo en el cual sucedió el evento |
| %DOMAIN%                         | De dominio                                          |
| %EVENT%                          | Evento                                              |
| %DESCR%                          | Descripción del evento                              |
| %RISE_TIME%                      | Hora de creación                                    |
| %KLCSAK_EVENT_TASK_DISPLAY_NAME% | Nombre de la tarea                                  |
| %KL_PRODUCT%                     | Agente de red                                       |
| %KL_VERSION%                     | Número de versión del Agente de red                 |
| %HOST_IP%                        | Dirección IP                                        |
| %HOST_CONN_IP%                   | Dirección IP de la conexión                         |

### 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.

En esta sección, encontrará información para utilizar, configurar y deshabilitar las novedades de Kaspersky.

## Acerca de las novedades de Kaspersky

La sección Anuncios de Kaspersky (**Control e informes** → **Anuncios de Kaspersky**) le mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center Linux y las aplicaciones administradas que están instaladas en los dispositivos administrados. Kaspersky Security Center Linux actualiza periódicamente la información de la sección, eliminando anuncios desactualizados y añadiendo nueva información.

Kaspersky Security Center Linux muestra solo los anuncios de Kaspersky relacionados con el Servidor de administración conectado 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. De forma predeterminada, los anuncios relacionados con seguridad están activados. Si no desea recibir estas novedades, [deshabilite la función correspondiente](#).

Para mostrarle la información que corresponde a la configuración de la protección de su red, Kaspersky Security Center Linux envía datos a los servidores en la nube de Kaspersky y recibe solo aquellos anuncios relacionados 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 podría ser útil para proteger sus dispositivos de red y en sus tareas diarias, Kaspersky Security Center Linux 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. Si no desea recibir anuncios, puede [desactivar esta función](#).

## 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 **Control e informes** → **Anuncios 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 **Control 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 [Anuncios de Kaspersky](#) (**Control e informes** → **Anuncios de Kaspersky**) le mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center Linux y las aplicaciones administradas que están 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**, seleccione la sección **Anuncios de Kaspersky**.
3. Ponga el conmutador en la posición **Los anuncios relacionados con la seguridad están desactivados**.
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 Activada**.

4. Haga clic en el botón **Guardar**.

Ya no recibirá novedades con fines publicitarios.

## Exportación de eventos a sistemas SIEM

En esta sección, se brindan instrucciones para configurar la exportación de eventos a un sistema SIEM.

### Escenario: Configurar la exportación de eventos a un sistema SIEM

Kaspersky Security Center Linux permite configurar la exportación de eventos a sistemas SIEM mediante uno de los siguientes métodos: exportación a cualquier sistema SIEM que utilice el formato Syslog o exportación de eventos a sistemas SIEM directamente desde la base de datos de Kaspersky Security Center Linux. Cuando completa este escenario, el Servidor de administración envía automáticamente eventos al sistema SIEM.

#### Requisitos previos

Antes de iniciar la exportación de la configuración de eventos en Kaspersky Security Center Linux:

- [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 de exportación de eventos al sistema SIEM consta de las siguientes etapas:

- **Configurar el sistema SIEM para recibir eventos de Kaspersky Security Center Linux**

Instrucciones: [Configurar la exportación de eventos en un sistema SIEM](#)

- **Seleccionar eventos que desea exportar al sistema SIEM**

Marque los eventos que desea exportar al sistema SIEM. Primero, [marque los eventos generales](#) que ocurren en todas las aplicaciones administradas de Kaspersky. A continuación, puede [marcar los eventos para aplicaciones Kaspersky administradas específicas](#).

- **Configuración de la exportación de eventos al sistema SIEM**

Puede exportar eventos usando uno de los siguientes métodos:

- [Utilizando los protocolos TCP/IP, UDP o TLS sobre TCP](#).
- Mediante una exportación de los eventos directamente [de 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

Después de configurar la exportación de eventos al sistema SIEM, puede ver los [resultados de la exportación](#) si seleccionó los eventos que desea exportar.

## Antes de comenzar

Al configurar la exportación automática de eventos en Kaspersky Security Center Linux, debe especificar ciertos parámetros de la configuración del sistema SIEM. Se recomienda que compruebe esta configuración de antemano a fin de prepararse para configurar Kaspersky Security Center Linux.

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 Linux y su servidor del sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center Linux y en la configuración del receptor de su sistema SIEM.

- **[Protocolo](#)** ⓘ

Protocolo usado para transferir mensajes desde Kaspersky Security Center Linux a su sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center Linux y en la configuración del receptor de su sistema SIEM.

## Acerca de la exportación de eventos

Kaspersky Security Center Linux 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.

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, por sus siglas en inglés).

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 exportar eventos desde Kaspersky Security Center Linux a sistemas SIEM externos involucra a dos partes: la que envía el evento, Kaspersky Security Center Linux, y un destinatario del evento, un 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 Linux. No importa cuál de los dos lados se configura primero. Puede configurar la transmisión de eventos desde Kaspersky Security Center Linux y, a continuación, configurar la recepción de eventos por parte del sistema SIEM o viceversa.

## Formato Syslog de exportación de eventos

Puede enviar eventos en formato Syslog a cualquier sistema SIEM. Usando el formato Syslog, puede transmitir cualquier evento que ocurra en el Servidor de administración y las aplicaciones de Kaspersky instaladas en dispositivos administrados. Al exportar eventos en formato Syslog, puede seleccionar exactamente qué tipos de eventos se transmitirán al sistema SIEM.

## Recepción de eventos por parte del sistema SIEM

El sistema SIEM debe recibir y analizar correctamente los eventos recibidos desde Kaspersky Security Center Linux. 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 exportar eventos desde Kaspersky Security Center Linux a sistemas SIEM externos involucra a dos partes: un remitente del evento, Kaspersky Security Center Linux y un destinatario del evento, el sistema SIEM. Debe configurar la exportación de eventos en su sistema SIEM y en Kaspersky Security Center Linux.

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 poder recibir los eventos enviados por Kaspersky Security Center Linux, debe configurar el receptor en su sistema SIEM. Por lo general, deberá especificar los valores de los siguientes parámetros dentro del sistema SIEM:

- **Protocolo de exportación**

Un protocolo de transferencia de mensajes, ya sea UDP, TCP o TLS sobre TCP. Este protocolo debe ser el mismo que el protocolo que especificó en Kaspersky Security Center Linux.

- **Puerto**

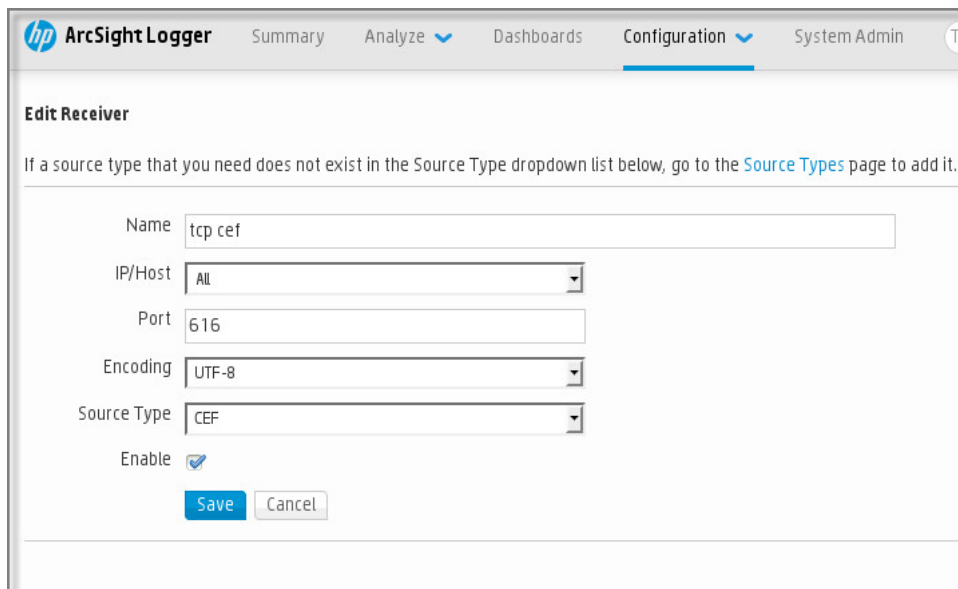
Número de puerto para conectar con Kaspersky Security Center Linux. Este puerto debe ser el mismo que [el puerto que especifica en Kaspersky Security Center Linux durante la configuración con un sistema SIEM](#).

- **Formato de los datos**

Especifique el formato Syslog.

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.



The screenshot shows the 'Edit Receiver' configuration page in the ArcSight Logger interface. The page has a navigation bar at the top with 'ArcSight Logger' and tabs for 'Summary', 'Analyze', 'Dashboards', 'Configuration', and 'System Admin'. Below the navigation bar, there is a heading 'Edit Receiver' and a note: 'If a source type that you need does not exist in the Source Type dropdown list below, go to the [Source Types](#) page to add it.' The configuration fields are: 'Name' (text input with 'tcp cef'), 'IP/Host' (dropdown menu with 'All'), 'Port' (text input with '616'), 'Encoding' (dropdown menu with 'UTF-8'), and 'Source Type' (dropdown menu with 'CEF'). There is an 'Enable' checkbox which is checked. At the bottom, there are 'Save' and 'Cancel' buttons.

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, parámetros, etcétera. Esto permite al sistema SIEM procesar eventos recibidos de Kaspersky Security Center Linux para 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

En esta sección, se brindan instrucciones para seleccionar los eventos que se exportarán en formato Syslog a un sistema SIEM.

## 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. Seleccione las casillas adyacentes a 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 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 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 ícono 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 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 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). Para exportar los eventos de Kaspersky Security Center Linux a sistemas externos, se utiliza el estándar [RFC 5424](#).

En Kaspersky Security Center Linux, puede usar el protocolo Syslog para configurar la exportación de los eventos a sistemas externos.

El proceso de exportación consta de dos pasos:

1. Habilitar la exportación de eventos automática. En este paso, Kaspersky Security Center Linux se configura para enviar eventos al sistema SIEM. Kaspersky Security Center Linux empieza a enviar eventos inmediatamente después de que usted activa 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.

## Configuración de Kaspersky Security Center Linux para la exportación de eventos a un sistema SIEM

Para exportar eventos al sistema SIEM, debe configurar el proceso de exportación en Kaspersky Security Center Linux.

*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 **SIEM**.

3. Haga clic en el enlace **Configuración**.

Se abre la sección **Exportar configuración**.

4. Ajuste la configuración en la sección **Exportar configuración**:

- **[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 Linux y su servidor del sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center Linux y en la configuración del receptor de su sistema SIEM.

- **[Protocolo](#)** 

Seleccione el protocolo que se utilizará para transferir mensajes al sistema SIEM. Puede seleccionar los protocolos TCP/IP, UDP o TLS over 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 recibir un archivo con la lista de certificados de una autoridad de certificados (CA) de confianza y cargar el archivo en Kaspersky Security Center Linux. Kaspersky Security Center Linux verifica si el certificado del servidor del sistema SIEM también está firmado por una CA de confianza o no.

Para añadir un certificado de confianza, haga clic en el botón **Busque archivo de certificados de CA** y, a continuación, cargue el certificado.

- **Huellas digitales SHA.** Puede especificar huellas digitales SHA-1 de certificados del sistema SIEM en Kaspersky Security Center Linux. Para agregar una huella digital SHA-1, cópiela en el campo **Huellas digitales** y haga clic en el botón **Añadir**.

Al usar el ajuste **Añadir autenticación del cliente**, puede generar un certificado para autenticar Kaspersky Security Center Linux. Por lo tanto, utilizará un certificado autofirmado emitido por Kaspersky Security Center Linux. En ese caso, podrá usar tanto un certificado de confianza como una huella digital SHA para autenticar al servidor del sistema SIEM.

- **Añadir Nombre del sujeto/Nombre alternativo del sujeto**

Se denomina "nombre del sujeto" al nombre de dominio para el que se ha obtenido un certificado. Kaspersky Security Center Linux no puede conectarse al servidor del sistema SIEM si el nombre de dominio del servidor del sistema SIEM no coincide con el nombre del sujeto del 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 **Añadir Nombre del sujeto/Nombre alternativo del sujeto** para especificar los nombres de sujeto pertinentes. Si alguno de los nombres de sujeto especificados coincide con el nombre de sujeto del certificado del sistema SIEM, Kaspersky Security Center Linux validará el certificado del servidor del sistema SIEM.

- **Añadir autenticación del cliente**

Para la autenticación del cliente, puede insertar su certificado o generarlo en Kaspersky Security Center Linux.

- **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.** Cargue un archivo con un certificado en el campo **Archivo con certificado** y un archivo con una clave privada en el campo **Archivo con clave**. 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 en Kaspersky Security Center Linux. Como resultado, Kaspersky Security Center Linux almacena el certificado autofirmado generado y puede pasar la parte pública del certificado o huella digital SHA1 al sistema SIEM.

5. Si lo desea, puede exportar eventos archivados desde la base de datos del Servidor de administración y establecer la fecha de inicio a partir de la cual desea iniciar la exportación de eventos archivados:

- a. Haga clic en el enlace **Establezca la fecha de inicio de la exportación.**
- b. En la sección que se abre, especifique la fecha de inicio en el campo **Fecha para iniciar la exportación.**
- c. Haga clic en el botón **Aceptar.**

6. Cambie la opción a la posición **Exportación automática de eventos a la base de datos del sistema SIEM activada.**

7. Haga clic en el botón **Guardar.**

La exportación al sistema SIEM queda configurada. Desde este momento, si configuró la recepción de eventos en un sistema SIEM, el Servidor de administración exportará [los eventos marcados](#) a un sistema SIEM. Si establece la fecha de inicio de la exportación, el Servidor de administración también exportará los eventos que haya marcado y que estén almacenados en la base de datos del Servidor de administración desde la fecha especificada.

## Exportación de eventos directamente desde la base de datos

Puede recuperar eventos directamente desde la base de datos de Kaspersky Security Center Linux sin necesidad de usar la interfaz de Kaspersky Security Center Linux. Puede enviar la solicitud directamente a las vistas públicas y recuperar los datos del evento o crear su propia vista sobre la base de vistas públicas existentes y dirigirse a ellas para obtener los datos que necesita.

### Vistas públicas

Para su comodidad, se proporciona un conjunto de vistas públicas en la base de datos de Kaspersky Security Center Linux. 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 vistas públicas correspondiente a otras entidades de Kaspersky Security Center Linux, por ejemplo, dispositivos, aplicaciones o usuarios. Puede usar esta información en sus consultas.

Esta sección contiene instrucciones para crear una consulta SQL mediante la utilidad klsq12 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 Linux, como el nombre de la instancia y el nombre de la base de datos.

## Creación de una consulta de SQL usando la utilidad klsql2

Esta sección describe cómo usar la utilidad klsql2 y cómo crear una consulta SQL usando esta utilidad. Utilice la versión de la utilidad klsql2 que se incluye en la versión de Kaspersky Security Center Linux instalada.

*Para usar la utilidad klsql2:*

1. Vaya al directorio `/opt/kaspersky/ksc64/sbin/ksql2` en el dispositivo que tiene instalado el Servidor de administración de Kaspersky Security Center.
2. En este directorio, cree el archivo en blanco `src.sql`.
3. Abra el archivo `src.sql` en cualquier editor de texto.
4. En el archivo `src.sql`, escriba la consulta SQL que desea, y luego guarde el archivo.
5. En el dispositivo con el Servidor de administración de Kaspersky Security Center instalado, en la línea de comandos, escriba el comando siguiente para ejecutar la consulta de SQL desde el archivo `src.sql` y guardar los resultados en el archivo `result.xml`:  

```
sudo ./ksql2 -i src.sql -u <nombre de usuario> -p <contraseña> -o result.xml
```

donde `<nombre de usuario>` y `<contraseña>` son credenciales de la cuenta de usuario que tiene acceso a la base de datos.
6. Si es necesario, ingrese el nombre de usuario y la contraseña de la cuenta de usuario que tiene acceso a la base de datos.
7. Abra el archivo `result.xml` creado recientemente para ver los resultados de la consulta.

Puede modificar el archivo `src.sql` y crear cualquier consulta para las vistas públicas. A continuación, desde la línea de comandos, ejecute su consulta 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, creada por medio de la utilidad klsql2.

El ejemplo siguiente ilustra la recuperación de eventos que ocurrieron en dispositivos durante los siete días anteriores, y muestra los eventos según la hora en la que se producen; los eventos más recientes se muestran primero.

### Ejemplo:

```
SELECT
e.nId, /* identificador del evento */
e.tmRiseTime, /* hora en la que ocurrió el evento */
e.strEventType, /* nombre interno del tipo de evento */
e.wstrEventTypeDisplayName, /* nombre mostrado del evento */
e.wstrDescription, /* descripción mostrada del evento */
e.wstrGroupName, /* nombre del grupo, donde se encuentra el dispositivo */
h.wstrDisplayName, /* nombre que se muestra del dispositivo en el que se produjo el
evento */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
```

```
CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* dirección IP del dispositivo en el
que se produjo el evento */
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
```

## La visualización del nombre de la base de datos de Kaspersky Security Center Linux

Si desea acceder a la base de datos de Kaspersky Security Center Linux por medio de las herramientas de administración de bases de datos SQL Server, MySQL o MariaDB, debe conocer el nombre de la base de datos a fin de conectarse desde su editor de scripts de SQL.

Ver el nombre de la base de datos de Kaspersky Security Center Linux:

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 **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 su sistema SIEM recibe y analiza correctamente los eventos enviados desde Kaspersky Security Center Linux, esto significa que la configuración en ambos lados se ha realizado bien. De lo contrario, compruebe que la configuración que especificó en Kaspersky Security Center Linux corresponda a la configuración de 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.

The screenshot shows the HP ArcSight Logger interface. At the top, there are browser tabs and a search bar. The main navigation menu includes Summary, Analyze (selected), Dashboards, Configuration, and System Admin. The search bar contains the query: `\_deviceGroup in ["mikrotik\_admin.avp.ru [tcp.cef]"]`. Below the search bar, a bar chart indicates 5 events scanned. A table of events is displayed with the following columns: Time (Event Time), Device, Logger, deviceVendor, deviceProduct, and deviceVersion. The table contains two rows of event data.

|   | Time (Event Time)       | Device                          | Logger | deviceVendor | deviceProduct  | deviceVersion |
|---|-------------------------|---------------------------------|--------|--------------|----------------|---------------|
| 1 | 2017/01/24 17:27:11 MSK | mikrotik_admin.avp.ru [tcp.cef] | Local  | KasperskyLab | SecurityCenter | 10.4.343      |
| 2 | 2017/01/24 17:26:41 MSK | mikrotik_admin.avp.ru [tcp.cef] | Local  | KasperskyLab | SecurityCenter | 10.4.343      |

Ejemplo de eventos

## Administración de revisiones de objetos

En esta sección encontrará información sobre la administración de revisiones de objetos. Kaspersky Security Center Linux le permite rastrear la modificación de objetos. 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:

- Servidores 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

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 **Descripción**. En la ventana **Descripción de la revisión del objeto**, puede agregar una descripción de revisión.

## 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

## 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 revisión**.
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.

## Eliminación de objetos

Esta sección proporciona información sobre la eliminación de objetos y la visualización de información sobre los objetos una vez que se eliminan.

Puede eliminar objetos como los siguientes:

- Directivas
- Tareas
- Paquetes de instalación
- Servidores de administración virtuales
- Usuarios
- Grupos de seguridad
- Grupos de administración

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**.

## Acerca 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 Linux 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. En este caso, 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](#) <sup>2</sup>.

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 Linux detecta el dispositivo durante el sondeo de red y lo añade 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.

## 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.

## Acerca de la eliminación de objetos de los repositorios de Cuarentena, Copia de seguridad o Amenazas activas

Cuando las aplicaciones de seguridad de Kaspersky instaladas en los dispositivos cliente colocan objetos en los repositorios de Cuarentena, Copia de seguridad o Amenazas activas, envían la información sobre los objetos añadidos a las secciones **Cuarentena**, **Copia de seguridad** o **Amenazas activas** en Kaspersky Security Center Linux. Cuando abre una de estas secciones, selecciona un objeto de la lista y hace clic en el botón **Eliminar**, Kaspersky Security Center Linux realiza una de las siguientes acciones o ambas acciones:

- Elimina el objeto seleccionado de la lista
- Elimina el objeto seleccionado del repositorio

La acción a realizar la define la aplicación de Kaspersky que colocó el objeto seleccionado en el repositorio. La aplicación de Kaspersky se especifica en el campo **Entrada añadida por**. Consulte la documentación de la aplicación de Kaspersky para obtener detalles sobre qué acción se realizará.

## Diagnóstico remoto de dispositivos cliente

Puede utilizar el diagnóstico remoto para la ejecución remota de 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 diagnósticos remotos en dispositivos cliente basados en Windows y Linux, primero 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 **Detección 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 **Diagnósticos remotos**.

Esto abre la ventana **Diagnósticos remotos** 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.

O bien, si necesita obtener toda la información de diagnóstico sobre un dispositivo cliente basado en Linux al mismo tiempo, 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 activar o desactivar el seguimiento.  
Se abre la lista de opciones de diagnóstico remoto.
4. Si desea habilitar el seguimiento, haga lo siguiente:
  - a. En la sección **Rastreo**, haga clic en **Activar rastreo**.
  - 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.

- [Rastreo basado en 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 los 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 **Activar rastreo** y **Modificar nivel de seguimiento** están desactivadas para este componente en los dispositivos cliente que ejecutan Linux.

5. Para desactivar el seguimiento para la aplicación seleccionada, haga clic en el botón **Desactivar rastreo**.  
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 de Xperf o deshabilitarlo:*

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.  
Aparecerá la lista de opciones de diagnóstico remoto para Kaspersky Endpoint Security para Windows.
4. En la sección **Rastreo de Xperf**, haga clic en **Activar rastreo de Xperf**.  
Si el seguimiento con Xperf ya está habilitado, verá, en cambio, el botón **Desactivar rastreo de Xperf**. Haga clic en este botón si desea desactivar el seguimiento de Xperf para Kaspersky Endpoint Security para Windows.
5. Cuando se abra la ventana **Cambiar nivel de seguimiento de 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 ligero** ⓘ

Un archivo de seguimiento de este tipo contiene una cantidad mínima de información sobre el sistema.

Esta opción está seleccionada de manera 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 manera predeterminada.

- [Tipo de 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 desactivar el seguimiento de Xperf para Kaspersky Endpoint Security para Windows, haga clic en **Desactivar rastreo de Xperf** en la sección **Rastreo de 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 desea descargar un archivo de seguimiento.

4. En la sección **Rastreo**, haga clic en el botón **Archivos de seguimiento**.

Se abre la ventana **Registros de rastreo 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 desea 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, el botón **Descargar una parte** se desactivará.

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 **Registros de instalación remota**, dependiendo de los archivos de seguimiento que desee eliminar.

El enlace **Registros de Windows Update** está disponible solo para dispositivos cliente basados en Windows.

Se abre la ventana **Registros de rastreo 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 archivos de seguimiento seleccionados quedan eliminados.

## 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 la aplicación**, haga clic en el botón **Descargar** para descargar información sobre la configuración de las aplicaciones instaladas en el dispositivo cliente.

El archivo ZIP con información se descarga en la ubicación que especifique.

## Descargar información del sistema desde un dispositivo cliente

*Para descargar información del sistema desde un dispositivo cliente:*

1. [Abra la ventana de diagnóstico remoto de un dispositivo cliente.](#)

2. En la ventana de diagnóstico remoto, seleccione la pestaña **Información del sistema**.

3. Haga clic en el botón **Descargar** para descargar la información del sistema sobre el dispositivo cliente.

Si obtiene información del sistema sobre un dispositivo basado en Linux, se añade al archivo obtenido un archivo de volcado para aplicaciones finalizadas de emergencia.

El archivo con la información se descarga en la ubicación especificada.

## 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 relevantes.

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 desactivará el botón **Descargar una parte**.

- b. En la ventana que se abre, especifique el nombre y la parte del registro que desee descargar.

Para dispositivos basados en Linux, no está disponible la edición del nombre de la parte del registro.

- c. Haga clic en **Descargar**.

El registro de eventos seleccionado, o una parte del mismo, se descarga en la ubicación que especifique.

## 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 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 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.

## Ejecutar los diagnósticos remotos del Agente de red de Kaspersky Security Center Linux y descargar los resultados

*Para iniciar el diagnóstico de Agente de red de Kaspersky Security Center Linux 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 Linux**.

Se abre la lista de opciones de diagnóstico remoto.

4. En la sección **Informe de diagnóstico**, haga clic en el botón **Ejecutar diagnósticos**.

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 un informe de diagnóstico**.

5. Haga clic en el botón **Descargar un informe de diagnóstico** para descargar el informe.

El informe se descarga en la ubicación especificada.

## Ejecutar una aplicación en un dispositivo cliente

Ocasionalmente, el personal técnico de Kaspersky puede pedirle que ejecute una aplicación en un 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 aplicaciones**, 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 ejecutará en un dispositivo remoto.

Puede especificar el nombre del archivo ejecutable y los argumentos de línea de comandos, si es necesario. Para ello, complete los campos **Archivo ejecutable almacenado en un archivo comprimido que se ejecutará en un dispositivo remoto** y **Argumentos de 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 de soporte de Kaspersky.

## Crear un archivo de volcado para una aplicación

Un archivo de volcado de la aplicación le permite ver los parámetros de la aplicación que se ejecuta en un dispositivo cliente en un momento dado. Este archivo también contiene información sobre los módulos que se cargaron para una aplicación.

La generación de archivos de volcado solo está disponible para procesos de 32 bits que se ejecutan en dispositivos cliente basados en Windows. Para dispositivos cliente que ejecutan Linux y para procesos de 64 bits, esta función no es compatible.

*Para 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 **Generar archivo de volcado para el proceso**, especifique el archivo ejecutable de la aplicación para la que desea generar un archivo de volcado.
4. Haga clic en el botón **Descargar** para guardar el archivo de volcado para la aplicación especificada.  
Si la aplicación especificada no se está ejecutando en el dispositivo cliente, se mostrará un mensaje de error.

## Ejecución de diagnósticos remotos en un dispositivo cliente basado en Linux

Kaspersky Security Center Linux le permite [descargar la información de diagnóstico básica desde un dispositivo cliente](#). O bien, 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 se debe diagnosticar y luego genera un archivo con la información de diagnóstico, la información del sistema sobre este dispositivo, los archivos de seguimiento de las aplicaciones, los registros del dispositivo y un archivo de volcado para aplicaciones finalizadas de emergencia.

Le recomendamos que utilice el script `collect.sh` para obtener toda la información de diagnóstico sobre el dispositivo cliente basado en Linux al mismo tiempo. Si descarga la información de diagnóstico de forma remota a través de Kaspersky Security Center Linux, 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 utilizando el script `collect.sh`, siga estos pasos:*

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 se debe diagnosticar.
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`.

# Administración de aplicaciones de terceros en dispositivos cliente

Esta sección describe las funciones de Kaspersky Security Center Linux relacionadas con la administración de aplicaciones de terceros que se ejecutan en dispositivos cliente.

## Escenario: Administración de aplicaciones

Puede administrar el inicio de aplicaciones en dispositivos de usuario. Puede permitir o impedir que ciertas aplicaciones se ejecuten en estos equipos. A esta funcionalidad la ejecuta el componente Control de aplicaciones. Solo podrá administrar aplicaciones instaladas en dispositivos Windows o Linux.

El componente Control de aplicaciones para sistemas operativos basados en Linux está disponible a partir de Kaspersky Endpoint Security 11.2 for Linux.

### Requisitos previos

- Kaspersky Security Center Linux se ha implementado en su organización.
- La directiva de Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security para Windows se crea y está activa.

### Etapas

El escenario de uso de Control de aplicaciones consta de etapas:

#### 1 Crear y ver la lista de aplicaciones instaladas en los dispositivos cliente

En esta etapa, descubrirá qué aplicaciones se encuentran instaladas en los dispositivos administrados. Podrá ver la lista de aplicaciones y decidir cuáles estarán permitidas y cuáles no bajo las políticas de seguridad de su organización. Las restricciones pueden estar vinculadas a las políticas de seguridad de la información de su organización. Si sabe exactamente cuáles son las aplicaciones instaladas en los dispositivos administrados, puede omitir esta etapa.

Instrucciones: [Obtener y ver una lista de aplicaciones instalada en dispositivos cliente](#)

#### 2 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. Si sabe exactamente qué archivos ejecutables están instalados en los dispositivos administrados, puede omitir esta etapa.

Instrucciones: [Obtener y ver una lista de archivos ejecutables almacenada en dispositivos cliente](#)

#### 3 Crear categorías de aplicaciones para el software utilizado en la organización

Analice las listas de aplicaciones y archivos ejecutables almacenados en los dispositivos administrados. Cree categorías de aplicaciones basadas en los resultados de este análisis. Recomendamos crear una categoría llamada "Aplicaciones de trabajo" que cubra las aplicaciones estándar que se utilicen en la organización. Luego, si tiene grupos de seguridad diferentes que trabajan con aplicaciones diferentes, puede crear una categoría de aplicaciones separada para cada grupo de seguridad.

Según el conjunto de criterios para crear una categoría de aplicaciones, puede crear categorías de aplicación de dos tipos.

Instrucciones: [Crear categoría de aplicación con contenido agregado manualmente](#), [Crear una categoría de aplicación que incluya archivos ejecutables de dispositivos seleccionados](#)

#### 4 Configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security

Configure el componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security for Linux utilizando las categorías de aplicaciones que creó en la etapa anterior.

Instrucciones: [Configuración de Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows](#).

#### 5 Activar el componente Control de aplicaciones en modo de prueba

Las reglas de Control de aplicaciones no deben bloquear las aplicaciones 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 este modo se encuentre activo, Kaspersky Endpoint Security para Windows no bloqueará las aplicaciones que las reglas de Control de aplicaciones no permitan iniciar, sino que simplemente notificará al Servidor de administración que tales aplicaciones se han ejecutado.

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 active la opción **Modo de prueba** en el proceso de configuración.

#### 6 Cambiar la configuración de las categorías de aplicaciones 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 de aplicaciones con contenido agregado manualmente que incluya los archivos ejecutables vinculados a los eventos de Control de aplicaciones.

Instrucciones: Kaspersky Security Center Web Console: [Agregar archivos ejecutables relacionados con eventos a la categoría de aplicación](#)

#### 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 de aplicaciones, 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 desactive la opción **Modo de prueba** en el proceso de configuración.

#### 8 Verificar la configuración de Control de aplicaciones

Asegúrese de haber hecho lo siguiente:

- Crear las categorías de aplicaciones.
- Configurar Control de aplicaciones con las categorías de aplicaciones.
- Aplicar las reglas de Control de aplicaciones en el modo de operación.

## Resultados

Al concluir este escenario, la ejecución de aplicaciones en los dispositivos administrados estará bajo su control. Los usuarios pueden iniciar solo aquellas aplicaciones que están permitidas en su organización y no pueden iniciar las que están prohibidas.

Para obtener información detallada acerca de Control de aplicaciones, consulte la [Ayuda de Kaspersky Endpoint Security for Linux](#) y [Kaspersky Endpoint Security para Windows](#).

## Acerca de Control de aplicaciones

El componente Control de aplicaciones supervisa los intentos de los usuarios de iniciar aplicaciones y regula dicho inicio mediante el uso de reglas de Control de aplicaciones.

El componente Control de aplicaciones está disponible para Kaspersky Endpoint Security 11.2 para Linux y versiones posteriores.

Cuando una aplicación no está alcanzada por una regla de Control de aplicaciones, la posibilidad de que se permita iniciarla depende del modo de funcionamiento del componente. Los modos disponibles son dos:

- *Lista de rechazados.* En este modo, se permite la ejecución de cualquier aplicación, excepto las que están alcanzadas por las reglas de bloqueo. Este modo está seleccionada de manera predeterminada.
- *Lista de admitidos.* En este modo, se impide la ejecución de todas las aplicaciones, excepto las que están alcanzadas por las reglas de autorización.

Las reglas de Control de aplicaciones se basan en categorías de aplicaciones. Estas categorías se crean sobre la base de criterios definidos por usted. En Kaspersky Security Center Linux, hay tres tipos de categorías de aplicaciones:

- [Categorías con contenido agregado de forma manual.](#) Defina condiciones, por ejemplo, metadatos de archivo, código hash de archivo, certificado de archivo y ruta de archivo, para incluir archivos ejecutables en la categoría.
- [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 acerca de Control de aplicaciones, consulte la [Ayuda de Kaspersky Endpoint Security for Linux](#) y [Kaspersky Endpoint Security para Windows](#).

## Obtener y ver una lista de aplicaciones instaladas en los dispositivos cliente

Kaspersky Security Center Linux 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.





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, nombre del proveedor, número de versión, lista de archivos ejecutables, lista de dispositivos en los que está instalada la aplicación.

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 sondeo**, 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:

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 acerca de Control de aplicaciones, consulte la [Ayuda de Kaspersky Endpoint Security for Linux](#) y [Kaspersky Endpoint Security para Windows](#).

## Obtención y visualización de una lista de archivos ejecutables almacenados en los dispositivos cliente

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.

En Kaspersky Endpoint Security for Linux, la función de inventario de archivos ejecutables está disponible desde la versión 11.2.

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 **Añadir**.  
Se inicia el [Asistente para crear nueva tarea](#). Siga los pasos del asistente.
3. En la página **Nueva tarea** de la lista desplegable **Aplicación**, seleccione Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security para Windows, según el sistema operativo de los dispositivos cliente.
4. Desde la lista desplegable **Tipo de tarea**, seleccione **Inventario**.
5. En la página **Finalizar la creación de tareas**, haga clic en el botón **Finalizar**.

Una vez que se completa el Asistente para crear nueva tarea, la tarea **Inventario** queda creada y configurada. 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 la [Ayuda de Kaspersky Endpoint Security for Linux](#) y la [Ayuda de Kaspersky Endpoint Security para Windows](#).

Una vez efectuada la tarea **Inventario**, se crea la lista de archivos ejecutables almacenados en los dispositivos administrados para que pueda verla.

Mientras se crea el inventario, se detectan los archivos ejecutables en los siguientes formatos: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, y HTML.

*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.

## 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 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 **Añadir**.  
Se inicia el Asistente para crear nueva categoría. Siga los pasos del asistente.
3. En la página del asistente **Seleccione el método de creación de la categoría**, especifique el nombre de la categoría de aplicación y seleccione la opción **Categoría con contenido añadido manualmente. Los datos de los archivos ejecutables se añaden manualmente a la categoría**.
4. En la página **Condiciones** del asistente, haga clic en el botón **Añadir** a fin de agregar un criterio de condición para incluir archivos en la categoría que se crea.
5. En la lista de la página **Criterios de condición**, seleccione el tipo de regla que desee usar para crear la categoría:

- [De 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. Los archivos ejecutables que se hayan firmado conforme a esos certificados se agregarán a la categoría personalizada.

- [Especificar la ruta a la aplicación \(se admiten máscaras\)](#) 

Seleccione esta opción para especificar la ruta a una carpeta del dispositivo cliente que contenga los archivos ejecutables que quiera agregar a la categoría de aplicaciones personalizada.

- [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. Puede seleccionar una aplicación de este registro y especificar los siguientes metadatos del archivo:

- 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.

- [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.

#### **Archivo 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 Linux calcule el valor de hash para archivos en esta categoría. La información sobre los valores hash calculados se almacena en la base de datos del Servidor de administración. Estos valores no ocupan una cantidad de espacio significativa en la base de datos.

SHA-256 es una función de hash criptográfica. En la actualidad, se la considera la más fiable en su clase, pues no se ha encontrado vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security para Linux es compatible con el cálculo de SHA-256.

Seleccione cualquiera de las opciones de cálculo del valor de hash de Kaspersky Security Center Linux para archivos en la categoría:

- Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security for Linux, marque la casilla **SHA-256**.
- Marque la casilla **Hash MD5** solo si utiliza Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Security para Linux no es compatible con la función hash MD5.

#### **Metadatos**

Seleccione esta opción si desea especificar los metadatos de los archivos (nombre, versión, proveedor, etc.). Los metadatos se enviarán al Servidor de administración. Los archivos ejecutables que contengan los metadatos especificados se agregarán a la categoría de aplicaciones.

#### **Certificado**

Seleccione esta opción para elegir certificados almacenados en el repositorio. Los archivos ejecutables que se hayan firmado conforme a esos certificados se agregarán a la categoría personalizada.

- [Desde la carpeta comprimida](#) 

Si esta opción está seleccionada, puede especificar un archivo de una carpeta archivada y luego seleccionar qué condición desea usar para añadir aplicaciones a la categoría de usuario. La carpeta archivada se descomprime y las condiciones que ha seleccionado se aplican a los archivos de la carpeta. Como condición, puede seleccionar uno de los siguientes criterios:

- **Archivo hash**

Usted selecciona qué función hash (MD5 o SHA-256) desea usar para calcular los valores hash. Las aplicaciones que tienen el mismo valor hash que los archivos de la carpeta archivada se añaden a la categoría aplicación de usuario.

Seleccione una función hash MD5 solo si utiliza Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Security para Linux no es compatible con la función hash MD5.

- **Metadatos**

Usted selecciona qué metadatos desea utilizar como criterio. Los archivos ejecutables que contienen los mismos metadatos se agregarán a la categoría de aplicaciones del usuario.

- **Certificado**

Seleccione qué propiedades del certificado (asunto del certificado, huella digital o emisor) desea utilizar como criterio. Los archivos ejecutables que se han firmado con los certificados que tienen las mismas propiedades se agregarán a la categoría de usuario.

Si esta opción está seleccionada, puede especificar un archivo de una carpeta archivada y luego seleccionar qué condición desea usar para añadir aplicaciones a la categoría de usuario. La carpeta archivada se descomprime y las condiciones que ha seleccionado se aplican a los archivos de la carpeta. Como condición, puede seleccionar uno de los siguientes criterios:

- **Archivo hash**

Usted selecciona qué función hash (MD5 o SHA-256) desea usar para calcular los valores hash. Las aplicaciones que tienen el mismo valor hash que los archivos de la carpeta archivada se añaden a la categoría aplicación de usuario.

Seleccione una función hash MD5 solo si utiliza Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Security para Linux no es compatible con la función hash MD5.

- **Metadatos**

Usted selecciona qué metadatos desea utilizar como criterio. Los archivos ejecutables que contienen los mismos metadatos se agregarán a la categoría de aplicaciones del usuario.

- **Certificado**

Seleccione qué propiedades del certificado (asunto del certificado, huella digital o emisor) desea utilizar como criterio. Los archivos ejecutables que se han firmado con los certificados que tienen las mismas propiedades se agregarán a la categoría de usuario.

El criterio seleccionado se agrega a la lista de condiciones.

Puede agregar tantos criterios como necesite para crear la categoría de aplicaciones.

6. En la página **Exclusiones** del asistente, haga clic en el botón **Añadir** a fin de agregar un criterio de condición exclusiva para excluir archivos en la categoría que se crea.

7. En la lista de la página **Criterios de condición**, seleccione un tipo de regla tal como lo hizo al elegir un tipo de regla para crear la categoría.

Cuando finaliza el asistente, 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 acerca de Control de aplicaciones, consulte la [Ayuda de Kaspersky Endpoint Security for Linux](#) y [Kaspersky Endpoint Security para Windows](#).

## 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 crear una categoría de aplicaciones 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 de aplicaciones.

2. Haga clic en el botón **Añadir**.

Se inicia el Asistente para crear nueva categoría. Siga los pasos del asistente.

3. En la página del asistente **Seleccione el método de creación de la categoría**, especifique el nombre de la categoría y seleccione la opción **Categoría que incluye archivos ejecutables de dispositivos seleccionados**. **Estos archivos ejecutables se procesan automáticamente y sus métricas se añaden a la categoría.**

4. Haga clic en **Añadir**.

5. En la ventana que se abre, seleccione el dispositivo que contenga los archivos ejecutables que desee usar para crear la categoría de aplicaciones. 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 Linux calcule el valor de hash para archivos en esta categoría. La información sobre los valores hash calculados se almacena en la base de datos del Servidor de administración. Estos valores no ocupan una cantidad de espacio significativa en la base de datos.

SHA-256 es una función de hash criptográfica. En la actualidad, se la considera la más fiable en su clase, pues no se ha encontrado vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security para Linux es compatible con el cálculo de SHA-256.

Seleccione cualquiera de las opciones de cálculo del valor de hash de Kaspersky Security Center Linux para archivos en la categoría:

- Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security for Linux, marque la casilla **SHA-256**.

Marque la casilla **Hash MD5** solo si utiliza Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Security para Linux no es compatible con la función hash MD5.

La casilla **Calcular SHA-256 para los archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)** está activada de forma 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 manera 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 manera 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 manera 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 de aplicaciones. La nueva categoría aparece en la lista de categorías de aplicaciones. Podrá usar la nueva categoría cuando configure Control de aplicaciones.

## Crear una categoría de aplicación que incluya archivos ejecutables de la 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 de aplicaciones 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 de aplicaciones.
2. Haga clic en el botón **Añadir**.  
Se inicia el Asistente para crear nueva categoría. Avance por el asistente utilizando el botón **Next**.
3. En la página **Seleccione el método de creación de la categoría** del Asistente, especifique el nombre de la categoría y seleccione la opción **Categoría que incluye archivos ejecutables de una carpeta específica. Los archivos ejecutables de las aplicaciones copiadas a la carpeta especificada se procesan automáticamente y sus métricas se añaden a la categoría**.
4. Especifique la carpeta con los archivos ejecutables que se utilizarán para crear la categoría de aplicaciones.
5. Defina los siguientes parámetros de configuración:
  - [Incluir bibliotecas de vínculo dinámico \(DLL\) 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 script 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 SHA-256 para archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores) / Calcular MD5 para 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 Linux calcule el valor de hash para archivos en esta categoría. La información sobre los valores hash calculados se almacena en la base de datos del Servidor de administración. Estos valores no ocupan una cantidad de espacio significativa en la base de datos.

SHA-256 es una función de hash criptográfica. En la actualidad, se la considera la más fiable en su clase, pues no se ha encontrado vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security para Linux es compatible con el cálculo de SHA-256.

Seleccione cualquiera de las opciones de cálculo del valor de hash de Kaspersky Security Center Linux para archivos en la categoría:

- Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security for Linux, marque la casilla **SHA-256**.

Marque la casilla **Hash MD5** solo si utiliza Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Security para Linux no es compatible con la función hash MD5.

La casilla **Calcular SHA-256 para los archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)** está activada de forma 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 el análisis de la carpeta en busca de cambios](#) 

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 manera predeterminada.



Cuando finaliza el asistente, se crea la categoría de aplicaciones. La nueva categoría aparece en la lista de categorías de aplicaciones. Puede usar la categoría de aplicaciones en la configuración del Control de aplicaciones.

Para obtener información detallada acerca de Control de aplicaciones, consulte la [Ayuda de Kaspersky Endpoint Security for Linux](#) y [Kaspersky Endpoint Security para Windows](#).

## Visualización de la lista de categorías de aplicaciones

Puede ver la lista de las categorías de aplicaciones configuradas y los parámetros 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 de aplicaciones.

*Para ver las propiedades de una categoría de aplicaciones:*

Haga clic en el nombre de la categoría de aplicaciones.

Se muestra la ventana de propiedades de la categoría de aplicaciones. Las propiedades se agrupan en varias pestañas.

## 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 **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 muestra la ventana **Control de aplicaciones** con la configuración de Control de aplicaciones.

4. La opción **Control de aplicaciones** está activada de forma predeterminada. Cambie el botón a **Control de aplicaciones DESACTIVADO** para deshabilitar la opción.

5. En la configuración del bloque **Configuración de Control de aplicaciones**, active el modo de operación 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, active el modo de prueba en la sección **Configuración de control de aplicaciones**. En el modo de prueba, 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 supervisa solo los módulos DLL y los controladores cargados después de seleccionarse la opción **Controlar la carga de módulos DLL**. Reinicie el equipo después de seleccionar la opción **Controlar la carga de módulos DLL** si desea que Kaspersky Endpoint Security para Windows supervise todos los módulos y controladores DLL, incluidos los cargados antes de que se inicie Kaspersky Endpoint Security para Windows.

7. (Opcional) En el bloque **Plantillas de mensajes**, cambie la plantilla del mensaje que se muestra cuando se bloquea el inicio de una aplicación y el mensaje de correo electrónico de la plantilla que se le envía.

8. En la configuración del bloque **Modo de control de aplicaciones**, seleccione el modo **Lista de rechazados** o **Lista de permitidos**.

De forma predeterminada, el modo **Lista de rechazados** está seleccionado.

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 **Añadir**.

Se abre la ventana **Regla de Control de aplicaciones**.

11. Haga clic en el enlace **Elija 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 **Control de aplicaciones**, en el bloque **Temas y sus derechos**, cree una lista de usuarios y grupos de usuarios para aplicar 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 acerca de Control de aplicaciones, consulte la [Ayuda de Kaspersky Endpoint Security for Linux](#) y [Kaspersky Endpoint Security para Windows](#).

## Agregar archivos ejecutables vinculados a eventos a una categoría de aplicaciones

Después de configurar Control de aplicaciones en las directivas de Kaspersky Endpoint Security, en la lista de eventos se mostrarán los eventos siguientes:

- **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 **Control 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. Avance por el asistente utilizando el botón **Next**.

4. En la página del asistente, especifique la configuración relevante:

- En la sección **Acción en el archivo ejecutable relacionado con el evento**, seleccione una de las siguientes opciones:

- [Añadir a una nueva categoría de aplicaciones](#)

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 manera predeterminada.

Si selecciona esta opción, escriba el nombre que tendrá la nueva categoría.

- [Añadir a una categoría de aplicaciones 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 regla**, seleccione una de las siguientes opciones:

- **Reglas para añadir inclusiones**

- **Reglas para añadir exclusiones**

- En la sección **Parámetro utilizado como condición**, seleccione una de las siguientes opciones:

- [Detalles del certificado \(o hashes SHA-256 para archivos sin certificado\)](#)

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 SHA-256. Si selecciona una función hash SHA-256, 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 SHA-256 de los archivos sin certificado) a las reglas de la categoría.

Esta opción está seleccionada de manera predeterminada.

- [Detalles del certificado \(se omitirán los archivos sin certificado\)](#)

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.

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 SHA-256 \(se omitirán los archivos sin hash\)](#)

Cada archivo tiene su propia función hash SHA-256. Si selecciona una función hash SHA-256, 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 SHA-256 del archivo ejecutable.

- [Solo MD5 \(modo discontinuado, solo para Kaspersky Endpoint Security 10 Service Pack 1\)](#) <sup>2</sup>

Seleccione esta opción solo si utiliza Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Security para Linux no admite una función hash MD5.

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).

##### 5. Haga clic en **Aceptar**.

Cuando finalice el asistente, los archivos ejecutables relacionados con los eventos de Control de aplicaciones se añaden a la categoría de aplicaciones existente o a una nueva categoría de aplicaciones. Puede ver la configuración de la categoría de aplicaciones creada o modificada.

Para obtener información detallada acerca de Control de aplicaciones, consulte la [Ayuda de Kaspersky Endpoint Security for Linux](#) <sup>2</sup> y [Kaspersky Endpoint Security para Windows](#) <sup>2</sup>.

# 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. Usted puede automatizar las tareas que no desee gestionar de forma manual. 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. Usando OpenAPI, puede desarrollar una aplicación cliente.

Puede usar el campo de búsqueda en la parte derecha de la pantalla para encontrar la información que necesita en la 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 "principal/secundario"](#), ejecutar [tareas](#) en Kaspersky Security Center Linux, 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 KIAkOAPI.tar.gz](#). Este archivo incluye el paquete KIAkOAPI y las muestras (puede copiarlas del archivo o de la guía de referencia de OpenAPI). El archivo KIAkOAPI.tar.gz también se encuentra en la carpeta de instalación de Kaspersky Security Center Linux.
2. [Instale el paquete KIAkOAPI](#) del archivo KIAkOAPI.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 KIAkOAPI.

Coincidencia entre escenarios de usuario y ejemplos de métodos OpenAPI de Kaspersky Security Center

| Ejemplo                                                               | Propuesta del ejemplo                                                                                                                                                                                                                                                                              | Escenario                                                                                                                             |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Registro KIAkParams</a>                                   | Puede extraer y procesar datos utilizando la estructura de datos KIAkParams. La muestra indica cómo trabajar con esta estructura de datos.<br><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                                                                                                                |
| <a href="#">Crear y eliminar una jerarquía "principal/secundario"</a> | Puede agregar un Servidor de administración secundario para establecer una jerarquía "principal/secundario". Alternativamente, puede desconectar de la jerarquía el Servidor de administración secundario.                                                                                         | <a href="#">Crear una jerarquía de Servidores de administración, agregar un Servidor de administración secundario, y eliminar una</a> |

|                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                           | <a href="#">jerarquía de Servidores de Administración</a>                           |
| <a href="#">Descargar archivos de lista de red a través de la puerta de enlace de conexión al host especificado</a>                                                  | Puede conectarse al agente de red en el dispositivo necesario utilizando una <a href="#">pasarela de conexión</a> y luego descargar un archivo con la lista de red a su dispositivo.                                                                                                                                                                                                                      | <a href="#">Ajuste de puntos de distribución y puertos de enlace de conexión</a>    |
| <a href="#">Instalar una clave de licencia almacenada en el repositorio del Servidor de administración principal en los servidores de administración secundarios</a> | 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                                             |
| <a href="#">Crear un informe de derechos de usuario efectivos</a>                                                                                                    | Puede crear <a href="#">diferentes informes</a> . 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><br>Puede descargar el informe en formato HTML, PDF o Excel.                                                                                               | <a href="#">Generación y visualización de un informe</a>                            |
| <a href="#">Iniciar la tarea del dispositivo</a>                                                                                                                     | Puede conectarse al Agente de red en el dispositivo necesario utilizando una <a href="#">pasarela de conexión</a> y luego ejecutar la tarea necesaria.                                                                                                                                                                                                                                                    | <a href="#">Iniciar una tarea manualmente</a>                                       |
| <a href="#">Registrar puntos de distribución para los dispositivos de un grupo</a>                                                                                   | Puede asignar dispositivos administrados como puntos de distribución (antes conocidos como agentes de actualización).                                                                                                                                                                                                                                                                                     | <a href="#">Actualización de las bases de datos y las aplicaciones de Kaspersky</a> |
| <a href="#">Enumerar todos los grupos</a>                                                                                                                            | Puede realizar varias acciones en los grupos de administración: El ejemplo muestra cómo hacer lo siguiente: <ul style="list-style-type: none"> <li>• Obtener un identificador del grupo raíz "Dispositivos administrados"</li> <li>• Moverse a través de la jerarquía de grupo</li> <li>• Recuperar la jerarquía completa y ampliada de los grupos, junto con sus nombres y nivel de anidación</li> </ul> | <a href="#">Configuración del Servidor de administración</a>                        |
| <a href="#">Enumerar las tareas, consultar las estadísticas de las tareas y ejecutar una tarea</a>                                                                   | Puede averiguar la siguiente información: <ul style="list-style-type: none"> <li>• Historial de progreso de la tarea.</li> <li>• Estado de la tarea actual.</li> <li>• Número de tareas en diferentes estados.</li> </ul> También puedes ejecutar una tarea. De forma predeterminada, la muestra ejecuta una tarea después de emitir sus estadísticas.                                                    | Supervisar la ejecución de tareas                                                   |
| <a href="#">Crear y ejecutar una tarea</a>                                                                                                                           | Puede crear una tarea. Especifique los siguientes parámetros de la tarea en la muestra:                                                                                                                                                                                                                                                                                                                   | Crear una tarea                                                                     |

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                              |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
|                                                        | <ul style="list-style-type: none"> <li>• Tipo.</li> <li>• Método de ejecución.</li> <li>• Nombre.</li> <li>• Grupo de dispositivos para el cual se utilizará la tarea.</li> </ul> <p>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 <a href="#">parámetros de tarea</a>.</p> |                                                                                              |
| <a href="#">Enumerar las claves de licencia</a>        | Puede obtener una lista de todas las claves de licencia activas para aplicaciones Kaspersky instaladas en dispositivos administrados de Administration Server. La lista contiene <a href="#">datos detallados</a> sobre cada clave de licencia, como un nombre, tipo o fecha de vencimiento.                                                                                                                                                                       | Visualización de información sobre las claves de licencia en uso                             |
| <a href="#">Crear y encontrar un usuario interno</a>   | Puede crear una cuenta para un trabajo adicional.                                                                                                                                                                                                                                                                                                                                                                                                                  | Seleccionar la cuenta para iniciar el Servidor de administración                             |
| <a href="#">Crear una categoría personalizada</a>      | Puede crear la categoría de aplicación con los <a href="#">parámetros</a> necesarios.                                                                                                                                                                                                                                                                                                                                                                              | <a href="#">Creación de una categoría de aplicaciones con contenido agregado manualmente</a> |
| <a href="#">Enumerar los usuarios mediante SrvView</a> | Puede usar la clase <a href="#">SrvView</a> para <a href="#">solicitar información detallada</a> 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 Linux a través de OpenAPI

Algunas aplicaciones interactúan con Kaspersky Security Center Linux 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 Linux a través de OpenAPI se conectan al Servidor de administración. Si ha configurado un [lista de direcciones IP permitidas](#) para conectarse al Servidor de administración, agregue las direcciones IP de los dispositivos donde están instaladas las aplicaciones que utilizan Kaspersky Security Center Linux OpenAPI. Para saber si una aplicación utiliza OpenAPI, consulte la ayuda de esa aplicación.



# Guía de dimensionamiento

Esta sección proporciona información sobre el dimensionamiento de Kaspersky Security Center Linux.

## Acerca de esta Guía

La Guía de dimensionamiento de Kaspersky Security Center Linux (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.

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
- 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

## 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.

## 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](#).

Servidor de administración, DBMS y Web Console, cada uno en un dispositivo separado, la red incluye 50 000 dispositivos

Configuración del dispositivo con el Servidor de administración instalado

| Hardware         | Valor                       |
|------------------|-----------------------------|
| CPU              | 8 núcleos, 2500 MHz         |
| RAM              | 16 GB                       |
| Disco duro       | 300 GB, RAID 10 recomendado |
| Adaptador de red | 1 Gbit                      |

La configuración del dispositivo que tiene DBMS instalado

| Hardware         | Valor                       |
|------------------|-----------------------------|
| CPU              | 16 núcleos, 2500 MHz        |
| RAM              | 32 GB                       |
| Disco duro       | 300 GB, RAID 10 recomendado |
| Adaptador de red | 1 Gbit                      |

La configuración del dispositivo que tiene Web Console instalado

| Hardware         | Valor               |
|------------------|---------------------|
| CPU              | 4 núcleos, 2500 MHz |
| RAM              | 8 GB                |
| Disco duro       | 40 GB               |
| Adaptador de red | 1 Gbit              |

Servidor de administración y Web Console en el mismo dispositivo, DBMS en un dispositivo separado, la red incluye 50 000 dispositivos

La configuración del dispositivo que tiene el Servidor de administración y Web Console instalados

| Hardware         | Valor                       |
|------------------|-----------------------------|
| CPU              | 12 núcleos, 2500 MHz        |
| RAM              | 24 GB                       |
| Disco duro       | 340 GB, RAID 10 recomendado |
| Adaptador de red | 1 Gbit                      |

La configuración del dispositivo que tiene DBMS instalado

| Hardware         | Valor                       |
|------------------|-----------------------------|
| CPU              | 16 núcleos, 2500 MHz        |
| RAM              | 32 GB                       |
| Disco duro       | 300 GB, RAID 10 recomendado |
| 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.

## 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:

$$(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), \text{ KB}$$

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.

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 necesario habitual del parámetro MAXSIZE para KAV\_log.LDF es de 20480 MB.

## Evaluación de espacio en el disco

El espacio en disco del Servidor de administración que se necesita para la carpeta `/var/opt/kaspersky/klnagnt_srv/` se puede calcular con la siguiente fórmula:

$$(724 * C + 0.15 * E + 0.17 * A), \text{KB}$$

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.

## 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 Linux crea un registro para esa VM dinámica en Kaspersky Security Center Web Console 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 Linux 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 Linux y de la base de datos del Servidor de administración y pueden, por ende, tener un impacto en el rendimiento de Kaspersky Security Center Linux y del DBMS. No recomendamos conectar más de 20 000 VM dinámicas a Kaspersky Security Center Linux.

Puede conectar más de 20 000 VM dinámicas a Kaspersky Security Center Linux 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 10 000 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.

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.

## 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.

## 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 pueden inundar la base de datos. En este caso, se recomienda seleccionar una de dos opciones en la configuración de la tarea:

- **Guardar eventos sobre 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 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 Linux.
- El registro del sistema operativo comienza a mostrar entradas sobre la eliminación automática de eventos cuando se excede el límite establecido sobre la cantidad 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 de la base de datos y las tareas de grupo para actualizar Kaspersky Endpoint Security son parte de la funcionalidad básica de Kaspersky Security Center Linux.

La tarea de inventario es parte de la función Administración de vulnerabilidades y parches y no está disponible si esta no está activada.



## 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 10 000               | 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 de la base de datos

El Servidor de administración deja de funcionar cuando se ejecutan las siguientes tareas:

- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de base de datos

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 del inventario del software

Puede reducir la carga a la que se somete la base de datos cuando se obtiene información sobre las aplicaciones instaladas. Para tal fin, recomendamos que ejecute una tarea de inventario 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 Linux 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.

## 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

| Escenario                                                                                                                                                                              | Tráfico del Servidor de administración hacia cada dispositivo administrado | Tráfico de cada dispositivo administrado al Servidor de administración |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|------------------------------------------------------------------------|
| Instalación de Kaspersky Endpoint Security for Linux 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 for Linux                                                                                                       | 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 <b>del Virus detectado</b> (1 virus)                                                                                       | 44 KB        | 50 KB       |
| Evento <b>del Virus detectado</b> (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 para Linux 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.

## Comunicarse con 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 Linux o en alguna de las fuentes de información sobre Kaspersky Security Center Linux, póngase en contacto con el Servicio de soporte técnico de Kaspersky. Los especialistas del Servicio de soporte técnico responderán a todas sus preguntas sobre la instalación y el uso de Kaspersky Security Center Linux.

Kaspersky proporciona soporte técnico a Kaspersky Security Center Linux durante su ciclo de vida (consulte la [página del ciclo de vida del soporte del producto](#)). 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](#).

## Fuentes de información acerca de la aplicación

### Página de Kaspersky Security Center Linux en el sitio web de Kaspersky

En la [página de Kaspersky Security Center Linux en el sitio web de Kaspersky](#), puede ver información general sobre la aplicación, sus funciones y características.

### La página de Kaspersky Security Center Linux 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 Linux en la Base de conocimientos](#), puede leer los 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 conocimientos pueden proporcionar respuestas a preguntas relacionadas tanto con Kaspersky Security Center Linux 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](#).

Dentro del foro, puede ver temas de discusión existentes, publicar comentarios y crear nuevos temas de discusión.

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](#).

## Problemas conocidos

Kaspersky Security Center Linux tiene una serie de limitaciones que no son críticas para el funcionamiento de la aplicación:

- Cuando importa la tarea *Descargar actualizaciones a los repositorios de puntos de distribución* o *Verificación de actualizaciones*, se activa 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 su red incluye un dominio de Microsoft Active Directory que contiene varias decenas de miles de objetos (dispositivos administrados, grupos de seguridad y cuentas de usuario) y el tamaño de la página de respuesta (el parámetro `MaxPageSize`) es menor que 5000, el sondeo del controlador de dominio no estará disponible y no recibirá información sobre los objetos de dominio. Cuando intenta sondear el controlador de dominio, se produce el error *Límite de tamaño excedido*. Aumentar el tamaño de la página de respuesta puede ayudar a corregir el error. Puede [usar la utilidad Ntdsutil.exe](#) para aumentar el valor del parámetro `MaxPageSize` a 5000 o 10 000, si es necesario.
- Cuando habilita KPSN en las propiedades del Servidor de administración y usa el puerto HTTPS 17111, la conexión con `ds.kaspersky.com` no se interrumpe.
- Kaspersky Endpoint Security para Windows no admite el servicio de proxy de KSN si la opción **Utilizar HTTPS** está habilitada en la configuración de proxy de KSN de las propiedades del Servidor de administración y la dirección del Servidor de administración contiene caracteres no latinos.
- Cuando cambia a un Servidor secundario desde la interfaz de un Servidor principal de administración de Kaspersky Security Center Linux, la sección **Actualizaciones sin interrupciones** del menú principal no se puede abrir.
- Cuando crea la tarea *Añadir clave* para Kaspersky Endpoint Security for Mac 11.3, el asistente muestra una tabla de claves de licencia que puede contener líneas vacías.
- El nivel de protección que se muestra en la directiva de Kaspersky Endpoint Security para Windows no se corresponde con el nivel de protección en la interfaz de Kaspersky Endpoint Security para Windows.
- Cuando ejecuta la tarea *Desinstalar aplicación en remoto* para eliminar una aplicación de Kaspersky de un dispositivo administrado, la tarea se completa correctamente, pero la aplicación no se elimina. Este problema es válido para Kaspersky Endpoint Security for Linux, Kaspersky Embedded Systems Security for Linux y Kaspersky Industrial CyberSecurity for Linux Nodes.
- La ventana de propiedades del Servidor de administración contiene configuraciones para dispositivos móviles, aunque Kaspersky Security Center Linux no admite la administración de dispositivos móviles.
- Si se ha detectado una aplicación de la sección **Registro de aplicaciones** en un dispositivo Linux, las propiedades de la aplicación no contienen información sobre los archivos ejecutables relacionados.
- Si instala el Agente de red en un dispositivo que ejecuta el sistema operativo ALT Linux a través de una tarea de instalación remota y ejecuta esta tarea en una cuenta con privilegios que no son root, la tarea falla. Ejecute la tarea de instalación remota en la cuenta raíz o cree y use un paquete de instalación independiente del Agente de red para instalar la aplicación localmente.
- En informes con formato de carta, un salto de página puede cortar una línea de texto horizontalmente.
- El asistente **Añadir 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 ha habilitado 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.

- 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.
- 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.
- En la edición Astra Linux de 64 bits, el paquete klnagent-astra no se puede actualizar con el paquete klnagent64\_14: se eliminará el paquete antiguo klnagent64-astra y el nuevo paquete klnagent64 se instalará en lugar de actualizarlo, por lo que se añadirá un nuevo ícono para el dispositivo con el paquete klnagent64\_14. Puede eliminar el icono anterior de este dispositivo.



# 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 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 Linux

La persona que administra las operaciones de la aplicación a través del sistema de administración centralizada remota de Kaspersky Security Center Linux.

## 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 Linux que permite la interacción entre el Servidor de administración y las aplicaciones de Kaspersky que se instalan 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 de un desarrollador externo o una aplicación Kaspersky que no admite la administración a través de Kaspersky Security Center Linux.

## Archivo de clave

Archivo de formato xxxxxxxx.key que hace posible usar una aplicación de Kaspersky con una licencia comercial o de prueba.

## 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.

## 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 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 suscripción adicional

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.

## 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. La Consola de administración es un análogo de Kaspersky Security Center Web 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.

## 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).

## Estación de trabajo del administrador

Un dispositivo desde el que se abre Kaspersky Security Center Web Console. Este componente proporciona una interfaz de administración de Kaspersky Security Center Linux.

La estación de trabajo del administrador se utiliza para configurar y administrar el lado del servidor de Kaspersky Security Center Linux. 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.

## 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.

## Grupo de roles

Un grupo de usuarios de dispositivos móviles Exchange ActiveSync a los que se les han otorgado los mismos [derechos de administrador](#).

## 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.

## 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 aplicaciones Kaspersky mediante servicios facilitados por Kaspersky Security Center Linux.

## 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)

Un componente de Kaspersky Security Center Linux diseñado para comprobar la capacidad de funcionamiento del sistema operativo en caso de la operación simultánea de Kaspersky Security Center Linux y de Microsoft NAP.

## 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

Conjunto de ajustes para [dispositivos móviles Exchange](#) que define su comportamiento cuando están conectados a un servidor Microsoft Exchange.

## 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.

## 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 dedicada al almacenamiento de información sobre eventos que ocurren en Kaspersky Security Center Linux.

## 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 equipos 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 Linux que almacena de forma centralizada la información sobre todas las aplicaciones Kaspersky que estén instaladas en la red de la empresa. 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 Linux diseñado para la administración del 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 web de Kaspersky Security Center Linux

Un componente de Kaspersky Security Center Linux 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.

## 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

Componente de Kaspersky Security Center Linux. 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.

## Usuarios internos

Las cuentas de los usuarios internos se utilizan para trabajar con Servidores de administración virtuales. Kaspersky Security Center Linux otorga los derechos de usuarios reales a los usuarios internos de la aplicación.

Las cuentas de los usuarios internos se crean y utilizan solo en Kaspersky Security Center Linux. No se transfiere ningún dato sobre estos usuarios internos al sistema operativo. Kaspersky Security Center Linux autentifica los usuarios internos.

## 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 el directorio 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.

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, Cisco Systems, IOS son marcas registradas o marcas comerciales de Cisco Systems, Inc. y sus filiales en los Estados Unidos y en otros países.

Citrix y XenServer son marcas comerciales de Citrix Systems, Inc. y/o de una o más de sus filiales y pueden estar registradas en la Oficina de Marcas y Patentes de los Estados Unidos y en 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.

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, Google Public DNS, Hangouts y YouTube son marcas comerciales de Google LLC.

EulerOS, FusionCompute y FusionSphere son marcas comerciales de Huawei Technologies Co., Ltd.

Intel, Core y Xeon son marcas comerciales de Intel Corporation en los Estados Unidos y/o en otros países.

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.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista y Windows Azure son marcas comerciales del grupo de compañías Microsoft.

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.

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.

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.

VMware, VMware vSphere y VMware Workstation son marcas comerciales registradas o marcas comerciales de VMware, Inc. en los Estados Unidos y/o en otras jurisdicciones.

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.