kaspersky

Kaspersky Security Center Cloud Console.

© 2025 AO Kaspersky Lab

Contenido

Ayuda de Kaspersky Security Center Cloud Console
Novedades
Kaspersky Security Center Cloud Console
- Acerca de Kaspersky Security Center Cloud Console
- Requisitos de hardware y software para Kaspersky Security Center Cloud Console
- Aplicaciones y soluciones de Kaspersky compatibles
- Localización de Kaspersky Security Center Cloud Console
- Comparación de Kaspersky Security Center y Kaspersky Security Center Cloud Console

Arquitectura y conceptos básicos
- Arquitectura
- Puertos utilizados por Kaspersky Security Center Cloud Console
- Conceptos básicos
  - Agente de red
  - Grupos de administración
  - Jerarquía de Servidores de administración
  - Servidor de administración virtual
  - Punto de distribución
  - Complemento web de administración
  - Directivas
  - Perfiles de directivas
  - Modo en que se relacionan las directivas y la configuración local de una aplicación

Licencias de la aplicación
- Licencias de Kaspersky Security Center Cloud Console
- Acerca del modo de prueba de Kaspersky Security Center Cloud Console
- Utilizar Kaspersky Marketplace para elegir soluciones empresariales de Kaspersky
- Licencias y la cantidad mínima de dispositivos para cada licencia
- Eventos sobre límites de licencia superados
- Métodos de distribución de los códigos de activación en los dispositivos administrados
- Añadir una clave de licencia del Servidor de administración
- 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
- Visualizar información acerca de las claves de licencia que están en uso en el repositorio del Servidor de administración
- Visualizar la información acerca de las claves de licencia utilizadas para una aplicación de Kaspersky específica
- Eliminación de una clave de licencia del Servidor de administración
- Eliminar una clave de licencia del repositorio
- Ver la lista de dispositivos donde una aplicación de Kaspersky no está activada
- Revocar la aceptación de un Contrato de licencia de usuario final
- Renovación de licencias para aplicaciones de Kaspersky
- Uso de Kaspersky Security Center Cloud Console después de la caducidad de la licencia
- Definiciones de licencia
  - Acerca de la licencia
  - Acerca del certificado de licencia
  - Acerca de la clave de licencia
  - Acerca del código de activación
  - Acerca de la suscripción

Provisión de datos
Datos que se envían a los servidores de Kaspersky
Datos necesarios para el funcionamiento del espacio de trabajo
Datos necesarios para el funcionamiento de las aplicaciones administradas
Datos de usuario procesados de forma local
Acerca de los documentos legales de Kaspersky Security Center Cloud Console
Guía de protección
Planificar la arquitectura de Kaspersky Security Center Cloud Console
Cuentas y autenticación
Gestión de la protección de dispositivos cliente
Configuración de la protección para aplicaciones administradas
Transferencia de eventos a sistemas de terceros
Recomendaciones de seguridad para sistemas de información de terceros
Recomendaciones para usar las aplicaciones de seguridad de Kaspersky
Interfaz de Kaspersky Security Center Cloud Console
Cambiar el idioma de la interfaz de Kaspersky Security Center Cloud Console
Cambiar la página de inicio de Kaspersky Security Center Cloud Console
Añadir y eliminar marcadores
Configuración inicial de Kaspersky Security Center Cloud Console
Administración de los espacios de trabajo
Acerca de la administración de los espacios de trabajo en Kaspersky Security Center Cloud Console
Guía de inicio rápido de Kaspersky Security Center Cloud Console
Creación de una cuenta
Registro de una empresa y creación de un espacio de trabajo
Proteger más de 10 000 dispositivos
Cómo abrir el espacio de trabajo de Kaspersky Security Center Cloud Console
Regreso a la lista de espacios de trabajo
Cerrar sesión en Kaspersky Security Center Cloud Console
Administración de la empresa y la lista de espacios de trabajo
Modificar información sobre una empresa y un espacio de trabajo.
Eliminar un espacio de trabajo y una empresa
Cancelar la eliminación de un espacio de trabajo
Administrar el acceso a la empresa y sus espacios de trabajo
Conceder acceso a su empresa y sus espacios de trabajo
Revocar el acceso a su empresa y sus espacios de trabajo
Restablecimiento de la contraseña
Modificación de la configuración de una cuenta en Kaspersky Security Center Cloud Console
Cambiar una dirección de correo electrónico
Cambiar una contraseña
Uso de la verificación de dos pasos
Acerca de la verificación de dos pasos
Escenario: configuración de la verificación de dos pasos
Configuración de la verificación de dos pasos por SMS
Configurar la verificación en dos pasos a través de una aplicación de autenticación
Cambio de su número de teléfono
Desactivación de la verificación de dos pasos
Eliminación de una cuenta en Kaspersky Security Center Cloud Console
Selección de los centros de datos usados para guardar información de Kaspersky Security Center Cloud Console

- Acceso a los servidores de DNS públicos

Escenario: creación de una jerarquía de servidores de administración administrados a través de Kaspersky Security Center Cloud Console

Migración a Kaspersky Security Center Cloud Console

- Acerca de la migración desde Kaspersky Security Center Web Console
  - Métodos de migración a Kaspersky Security Center Cloud Console
  - Escenario: Migración sin una jerarquía de Servidores de administración
  - Asistente de migración
    - Paso 1. Exportación de dispositivos administrados, objetos y configuraciones administradas desde Kaspersky Security Center Web Console
    - Paso 2. Importación del archivo de exportación en Kaspersky Security Center Cloud Console
    - Paso 3. Reinstalación del Agente de red en dispositivos administrados a través de Kaspersky Security Center Cloud Console
  - Migración con una jerarquía de Servidores de administración
  - Escenario: migración de dispositivos con sistemas operativos Linux o macOS
  - Escenario: Migración inversa de Kaspersky Security Center Cloud Console a Kaspersky Security Center
  - Migración con Servidores de administración virtuales
    - Escenario: migración con servidores de administración virtuales mediante el traslado de dispositivos
    - Escenario: migración manual con servidores de administración virtuales
    - Escenario: mover dispositivos desde los grupos de administración bajo la administración de servidores virtuales
- Acerca de la migración de Pro View a Expert View:

Asistente de inicio rápido

- Acerca del asistente de inicio rápido
- Inicio del asistente de inicio rápido
- Paso 1. Seleccionar paquetes de instalación para descargar
- Paso 2. Configuración de un servidor proxy
- Paso 3. Configurar Kaspersky Security Network
- Paso 4. Configuración de la administración de actualizaciones de terceros
- Paso 5. Creación de una configuración básica de protección de la red
- Paso 6. Cerrar el asistente de inicio rápido

Despliegue inicial de las aplicaciones de Kaspersky

- Escenario: despliegue inicial de aplicaciones de Kaspersky
- Crear paquetes de instalación para aplicaciones de Kaspersky.
- Distribución de paquetes de instalación a servidores de administración secundarios
- Crear un paquete de instalación independiente para el Agente de red
- Ver la lista de paquetes de instalación independientes
- Crear un paquete de instalación personalizado
- Requisitos para un punto de distribución
- Ajustes del paquete de instalación del Agente de red
- Infraestructura virtual
  - Sugerencias sobre la reducción de la carga en máquinas virtuales
  - Compatibilidad con máquinas virtuales dinámicas
  - Soporte de copia de máquinas virtuales
- Uso del Agente de red para Windows, Linux y macOS: comparación
- Definir ajustes para instalaciones remotas en dispositivos Unix
- Reemplazo de aplicaciones de seguridad de terceros
- Opciones para la instalación manual de aplicaciones
- Despliegue forzado con la tarea de instalación remota de Kaspersky Security Center Cloud Console
- Asistente de despliegue de la protección

Paso 1. Iniciar Asistente de despliegue de la protección
Paso 1. Seleccionar el paquete de instalación
Paso 2. Seleccionar la versión del Agente de red
Paso 3. Seleccionar los dispositivos
Paso 4. Configurar la tarea de instalación remota
Paso 5. Opciones de reinicio
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
Configuración de la red para interactuar con servicios externos
Preparación de un dispositivo que ejecuta Astra Linux en el modo de entorno de software cerrado para la instalación del Agente de red
Preparación de un dispositivo Linux e instalación del Agente de red en un dispositivo Linux de forma remota
Instalar aplicaciones mediante una tarea de instalación remota
Instalación de una aplicación de forma remota
Instalar aplicaciones en los Servidores de administración secundarios
Inicio y detención de aplicaciones de Kaspersky
Administración de dispositivos móviles
Capacidades de detección y respuesta
Acerca de las capacidades de detección y respuesta
Cambios en la interfaz después de integrar las funciones de detección y respuesta
Descubrir dispositivos en red y crear grupos de administración
Escenario: Descubrir dispositivos conectados a la red
Sondeo de red
Sondeo de la red de Windows
Sondeo del controlador de dominio
Sondeo de intervalos IP
Configuración de un controlador de dominio Samba
Agregar y modificar un intervalo IP
Ajuste de puntos de distribución y puertas de enlace de conexión
Cálculo de la cantidad de puntos de distribución y su configuración
Configuración estándar de puntos de distribución: oficina única
Configuración estándar de puntos de distribución: varias oficinas remotas pequeñas
Designación manual de puntos de distribución
Modificar la lista de puntos de distribución para un grupo de administración
Uso de un punto de distribución como servidor push
Uso de la opción "No desconectarse del Servidor de administración" para proporcionar conectividad continua entre un dispositivo administrado y el Servidor de administración
Creación de grupos de administración
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
Configuración de reglas de retención para dispositivos no asignados
Configurar la protección de la red
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
Ajustes de la directiva del Agente de red
Comparación de la configuración de la directiva 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
Excluir detalles de software de la memoria del Servidor de administración
Configurar el registro de eventos de directiva importantes en la base de datos del Servidor de administración
Configuración manual de la tarea de grupo para actualizar Kaspersky Endpoint Security
Tareas
Acerca de las tareas
Acerca del alcance de las tareas
Crear una tarea
Ver la lista de tareas
Iniciar una tarea manualmente
Iniciar una tarea para los dispositivos seleccionados
Configuración y propiedades generales de las tareas
Exportar una tarea
Importar una tarea
Ver resultados de la ejecución de tareas almacenados en el Servidor de administración
Administración de dispositivos cliente
Configuración de un dispositivo administrado
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
Ver y configurar las acciones para dispositivos inactivos
Acerca de los estados de los dispositivos
Configurar cambios de estado para los dispositivos
Cambiar los dispositivos cliente de Servidor de administración
Evitar conflictos entre varios Servidores de administración
Crear perfiles de conexión al Servidor de administración
Acerca de los clústeres y las matrices de servidores
Propiedades de un clúster o matriz de servidores
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 dispositivos manualmente
Quitar etiquetas asignadas 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
Cuarentena y Copia de seguridad
Descargar un archivo desde los repositorios
Eliminar archivos de los repositorios
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
Realizar un diagnóstico remoto de una aplicación y descargar los resultados
Ejecutar una aplicación en un dispositivo cliente
Crear un archivo de volcado para una aplicación
Conexión remota al escritorio de un dispositivo cliente
Conectarse a un dispositivo a través de Windows Desktop Sharing
Activación de reglas en modo Aprendizaje inteligente
Cómo ver la lista de detecciones realizadas con las reglas del Control de anomalías adaptativo
Adición de exclusiones para las reglas del Control de anomalías adaptativo
Administrar grupos de administración
Creación de grupos de administración
Instalación automática de aplicaciones en dispositivos de un grupo de administración
Traslado de grupos de administración
Eliminación de grupos de administración
Directivas y perfiles de directivas
Acerca de las directivas
Acerca del candado y el bloqueo de ajustes
Herencia en las directivas y los perfiles de directivas
Jerarquía de directivas
Perfiles de directivas en una jerarquía de directivas
Cómo se implementan los valores de configuración en un dispositivo administrado
Administración de directivas
Ver la lista de directivas
Crear una directiva
Modificar una directiva
Ajustes generales de una directiva
Habilitar y deshabilitar una opción de herencia en las directivas
Copiar una directiva
Mover una directiva
Exportación de una directiva
Importación de una directiva
Ver el gráfico de distribución de una directiva
Activar una directiva automáticamente ante un brote de virus
Sincronización forzada
Eliminar una directiva

- Administración de perfiles de directivas
  - Ver los perfiles de una directiva
  - Cambiar la prioridad de un perfil de directiva
  - Crear un perfil de directiva
  - Modificar un perfil de directiva
  - Copiar un perfil de directiva
  - Crear una regla de activación para un perfil de directiva
  - Eliminar un perfil de directiva
- Protección y cifrado de datos
  - Ver la lista de unidades cifradas
  - Crear y visualizar informes sobre cifrado
  - Brindar acceso a una unidad cifrada en modo sin conexión
- Usuarios y roles de usuario
  - Acerca de las cuentas de usuario
  - Agregar una cuenta de un usuario interno
  - 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 de seguridad
  - Asignación de un rol a un usuario o 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
  - Creación de un grupo de seguridad
  - Edición de un grupo de seguridad
  - Agregar cuentas de usuario a un grupo interno
  - Eliminar un grupo de seguridad
  - Configuración de la integración de ADFS
  - Configuración de la integración con Microsoft Entra ID
    - Cómo activar el sondeo de Microsoft Entra ID
    - Añadir Kaspersky Security Center Cloud Console a la lista de aplicaciones
  - Designación de un usuario como propietario de un dispositivo
  - Asignar a un usuario como propietario del dispositivo tras instalar el Agente de red
- Administración de revisiones de objetos
  - Reversión de cambios
  - Agregar una descripción a una revisión
  - Ver y guardar una revisión de la directiva
- Kaspersky Security Network (KSN)
  - Acerca de 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
- Eliminación de objetos

Actualización de las bases de datos y las aplicaciones de Kaspersky
Escenario: actualización periódica de las 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 una tarea para descargar las actualizaciones en los repositorios de los puntos de distribución
Configuración de los dispositivos administrados para recibir actualizaciones solo desde los puntos de distribución
Habilitación y deshabilitación de actualizaciones automáticas y parches para componentes de Kaspersky Security Center Cloud Console
Instalación automática de actualizaciones para Kaspersky Endpoint Security para Windows
Acerca de los estados de actualización
Aprobar y rechazar actualizaciones de software
Usar archivos diff para actualizar las bases de datos y los módulos de software de Kaspersky
Actualizar las bases de datos y los módulos de software de Kaspersky en dispositivos sin conexión
Actualización de las bases de datos de Kaspersky Security for Windows Server
Administración de aplicaciones de terceros en dispositivos cliente
Limitaciones de Administración de vulnerabilidades y parches
Disponibilidad de funciones Administración de vulnerabilidades y parches en modo comercial y de prueba y bajo varias opciones de licencia
Acerca de las aplicaciones de terceros
Actualizaciones para el software de terceros
Escenario: Actualización de software de terceros
Instalación de actualizaciones para el software de terceros
Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas
Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas
Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades
Agregar reglas de instalación de actualizaciones
Crear la tarea Instalar actualizaciones de Windows Update
Ver información sobre las actualizaciones disponibles para el software de terceros
Exportar la lista de actualizaciones de software disponibles a un archivo
Aprobar y rechazar actualizaciones de software de terceros
Actualización automática de aplicaciones de terceros
Encontrar y corregir vulnerabilidades de software
Reparación de vulnerabilidades de software
Crear la tarea Reparar vulnerabilidades
Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades
Agregar reglas de instalación de actualizaciones
Ver información sobre las vulnerabilidades de software detectadas en todos los dispositivos administrados
Ver información sobre las vulnerabilidades de software detectadas en un dispositivo administrado específico
Ver estadísticas de las vulnerabilidades presentes en los dispositivos administrados
Exportar la lista de vulnerabilidades de software a un archivo
Ignorar vulnerabilidades de software
Escenario: encontrar y corregir vulnerabilidades de software
Configurar el período máximo de almacenamiento para la información sobre las vulnerabilidades reparadas
Administración de las aplicaciones que se ejecutan en los dispositivos cliente
Uso de Control de aplicaciones para administrar archivos ejecutables
Modos y categorías de Control de aplicaciones
Obtener y ver una lista de aplicaciones instaladas en los dispositivos cliente
Obtener y ver una lista de archivos ejecutables instalada en dispositivos cliente
Crear una categoría de aplicaciones con contenido agregado manualmente
Crear una categoría de aplicaciones con archivos ejecutables de dispositivos específicos

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
Crear un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky
Ver y modificar la configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky
Configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky
Etiquetas de aplicación
Creación de una etiqueta de aplicación
Cambiar el nombre de una etiqueta de aplicación
Asignación de etiquetas a una aplicación
Quitarle una etiqueta a una aplicación
Eliminación de una etiqueta de aplicación
Configuración del Servidor de administración
Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario
Configuración del plazo de almacenamiento de eventos relacionados con los dispositivos eliminados
Agrupación de mensajes de correo electrónicos sobre eventos
Limitaciones en la administración de Servidores de administración secundarios que se ejecutan de forma local a través de Kaspersky Security Center Cloud Console
Ver la lista de servidores de administración secundarios
Eliminar una jerarquía de servidores de administración
Configuración de la interfaz
Administración de servidores de administración virtuales
Crear un Servidor de administración virtual
Habilitación y deshabilitación de un Servidor de administración virtual
Asignar un administrador para un Servidor de administración virtual
Eliminación de un Servidor de administración virtual
Supervisión e informes
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 de Kaspersky Security Center Cloud Console

Eventos de los componentes de Kaspersky Security Center Cloud Console
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 Fallo operativo
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 Fallo operativo
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
Registro de información sobre eventos para tareas y directivas
Eliminar eventos
Eliminación de selecciones de eventos
Notificaciones y estados de los dispositivos
Acerca de las notificaciones
Configurar cambios de estado para los dispositivos
Configurar el envío de notificaciones
Novedades de Kaspersky
Acerca de las novedades de Kaspersky
Dejar de recibir las novedades de Kaspersky
Recepción de una advertencia de caducidad de la licencia
Cloud Discovery
Activar Cloud Discovery mediante el widget
Cómo añadir el widget de Cloud Discovery al panel
Visualizar información sobre el uso de servicios en la nube
Nivel de riesgo de un servicio en la nube
Bloquear el acceso a servicios en la nube no deseados
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
Realizar un diagnóstico remoto de una aplicación 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
Exportación de eventos a sistemas SIEM
Configurar la exportación de eventos a sistemas SIEM
Antes de comenzar
Acerca de la exportación de eventos
Configuración de la exportación de eventos en un sistema SIEM
Marcar los eventos que se exportarán a un sistema SIEM en formato Syslog
Marcar eventos de una aplicación de Kaspersky para 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 Cloud Console para exportar eventos al sistema SIEM
Ver los resultados de la exportación
Guía de inicio rápido para proveedores de servicios administrados (MSP)
Acerca de Kaspersky Security Center Cloud Console
Características clave de Kaspersky Security Center Cloud Console
Acerca de las licencias de Kaspersky Security Center Cloud Console para los MSP
Acerca de las capacidades de detección y respuesta para MSP
Guía de inicio rápido de Kaspersky Security Center Cloud Console
Recomendaciones para administrar los dispositivos de sus clientes
Esquema de despliegue típico para MSP
Escenario: Despliegue de la protección (administración de inquilinos a través de los Servidores de administración virtual)
Escenario: Despliegue de la protección (administración de inquilinos a través de los grupos de administración)
Uso conjunto de Kaspersky Security Center y Kaspersky Security Center Cloud Console
Licencias de aplicaciones de Kaspersky para los MSP
Capacidades de supervisión e informes para los MSP
Trabajo con Kaspersky Security Center Cloud Console en un entorno de nube
Opciones de licencia en un entorno de nube
Preparación para trabajar en un entorno de nube a través de Kaspersky Security Center Cloud Console
Trabajar en el entorno de nube de Amazon Web Services
Acerca del trabajo con el entorno de nube de Amazon Web Services
Creación de cuentas de usuario de IAM para instancias de Amazon EC2
Asegurarse de que el Servidor de administración de Kaspersky Security Center Cloud Console tiene los permisos para funcionar con AWS
Crear una cuenta de usuario de IAM para trabajar con Kaspersky Security Center Cloud Console
Trabajar en el entorno de nube de Microsoft Azure
Acerca del uso de Microsoft Azure
Creación de una suscripción, un id. de aplicación y una contraseña
Asignación de una función al id. de la aplicación en Azure
Trabajar con Google Cloud
Asistente de configuración del entorno de nube en Kaspersky Security Center Cloud Console
Paso 1. Comprobar los complementos y paquetes de instalación necesarios
Paso 2. Selección del método de activación de la aplicación
Paso 3. Selección del entorno de nube y autorización
Paso 4. Sondeo de segmentos y configuración de la sincronización con la nube
Paso 5. Seleccionar una aplicación para crear una directiva y tareas para
Paso 6. Configuración de Kaspersky Security Network para Kaspersky Security Center Cloud Console
Paso 7. Creación de una configuración de protección inicial

Sondeo de segmentos de red a través de Kaspersky Security Center Cloud Console
Añadir conexiones para el sondeo de segmentos de la nube a través de Kaspersky Security Center Cloud Console
Eliminar conexiones para el sondeo de segmentos de nube
Configuración de la programación de sondeo a través de Kaspersky Security Center Cloud Console
Ver los resultados del sondeo del segmento de la nube a través de Kaspersky Security Center Cloud Console
Ver las propiedades de dispositivos de la nube a través de Kaspersky Security Center Cloud Console
Sincronización con la nube: Configuración de la regla de movimiento
Instalación remota de aplicaciones en máquinas virtuales de Azure
Ponerse en contacto con el Soporte técnico
Cómo obtener soporte técnico
Consultas mediante Kaspersky CompanyAccount al servicio de soporte técnico
Información necesaria para los especialistas del Soporte Técnico de Kaspersky
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 Cloud Console
Agente de autenticación
Agente de red
Aplicación incompatible
Archivo de clave
Bases de datos antivirus
Brote de virus
Clave activa
Clave de acceso de AWS IAM
Clave de licencia adicional (o de reserva)
Cloud Discovery
Complemento web de administración
Configuración de la tarea
Configuración de programa
Consola de administración de AWS
Cuarentena
Cuenta en Kaspersky Security Center Cloud Console
Directiva
Dispositivo administrado
Dispositivo con protección de UEFI
Dominio de difusión
Espacio de trabajo
Estado de protección
Estado de protección de la red
Etiqueta de aplicación
Etiqueta del dispositivo
Función de IAM
Gravedad de un evento
Grupo de administración

HTTPS
Identity and Access Management (IAM)
Imagen de máquina de Amazon (AMI)
Instalación forzada
Instalación local
Instalación remota
Instancia de Amazon EC2
Interfaz de programación de aplicaciones de AWS (API de AWS)
JavaScript
Kaspersky Next Expert View
Kaspersky Private Security Network (KPSN)
Kaspersky Security Network (KSN)
Lightweight Nagent (LWNGT)
Network Location Awareness (NLA)
Nivel de importancia del parche
Operador de Kaspersky Security Center Cloud Console
Paquete de instalación
Perfil de directiva
Periodo de vigencia de la licencia
Propietario del dispositivo
Protección antivirus para redes
Puerta de enlace de conexión
Punto de distribución
Repositorio de eventos
Restauración
Servidor de administración
Servidor de administración doméstico
Servidor de administración virtual
Servidores de actualizaciones de Kaspersky
SSL
Tarea
Tarea de grupo
Tarea local
Tarea para dispositivos específicos
Umbral de actividad viral
Usuario de IAM
Vulnerabilidad
Zona desmilitarizada (DMZ)
Información sobre el código de terceros
Avisos de marcas registradas

Ayuda de Kaspersky Security Center Cloud Console

	Novedades Descubra las novedades de la última versión de la aplicación.		**Configurar la protección de la red** Administre la seguridad de una organización configurando las directivas y tareas de las aplicaciones de Kaspersky de acuerdo con los requisitos de la organización.
	Requisitos de hardware y software Compruebe qué sistemas operativos y versiones de aplicaciones son compatibles.		**Aplicaciones de Kaspersky: actualización regular de las bases de datos y los módulos de software** Mantenga la fiabilidad del sistema de protección.
	Licencias de Kaspersky Security Center Cloud Console Obtenga más información sobre el funcionamiento de Kaspersky Security Center Cloud Console en el modo de prueba y en el modo comercial		**Supervisión e informes** Vea su infraestructura, los estados de protección de los dispositivos en red y las estadísticas para administrar el estado actual de protección de su organización. También puede usar informes.
	Configuración inicial Comience a trabajar con su espacio de trabajo, configure Kaspersky Security Center Cloud Console según sus necesidades.		**Administración de vulnerabilidades y parches** Busque y corrija vulnerabilidades en las aplicaciones de otros desarrolladores.
	Migración a Kaspersky Security Center Cloud Console Migre sus grupos de administración y objetos relacionados existentes de Kaspersky Security Center en las instalaciones a Kaspersky Security Center Cloud Console.		**Exportación de eventos a sistemas SIEM** Configura la Exportación de eventos a sistemas SIEM mediante el protocolo Syslog.
	Descubrimiento de dispositivos conectados a la red Descubra los dispositivos existentes y nuevos en la red de su organización.		**Trabajo en un entorno de nube** Protege máquinas virtuales en entornos de nube: Amazon Web Services™, Microsoft Azure™, Google™ Cloud Platform.
	Ajuste de puntos de distribución y/o puertas de enlace de conexión Configure sus puntos de distribución.		**Guía de inicio rápido para proveedores de servicios gestionados (MSP)** Aprenda cómo trabajar con Kaspersky Security Center Cloud Console, si es administrador de MSP.
	Aplicaciones de Kaspersky: despliegue centralizado Despliegue aplicaciones de Kaspersky.		

Novedades

Actualización de abril de 2025

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes mejoras:

- Kaspersky Security Center Cloud Console ahora admite las siguientes aplicaciones de Kaspersky:
  - Kaspersky Embedded Systems Security 3.4 para Linux
  - Kaspersky Endpoint Security 12.2 para Linux
  - Kaspersky Endpoint Security 12.8 for Windows
- Cargue y ejecute una aplicación (o script) para realizar diagnósticos en un dispositivo administrado. Ahora puede cargar la carpeta o el archivo comprimido que contiene el archivo ejecutable, o directamente el archivo ejecutable. Una vez ejecutada correctamente la aplicación, puede descargar los resultados de la ejecución.
- La información sobre los usuarios que en un momento dado están conectados al dispositivo administrado ahora se muestra en la sección **General** → **Sesiones** de la ventana de propiedades del dispositivo.
- Nuevo idioma compatible: la infraestructura de Kaspersky Security Center Cloud Console está disponible en el idioma chino simplificado.
- Mejoras en la experiencia del usuario:
  - Los paquetes de instalación disponibles se muestran en una pestaña.
  - Puede cambiar la configuración de la página de inicio a través de la nueva sección **Enlaces rápidos**. De forma predeterminada, la pestaña **Ajustes de la página de inicio** de la sección **Enlaces rápidos** se establece como página de inicio.
  - Se realiza una actualización de la navegación a través de los grupos de administración: puede ir al subgrupo requerido haciendo clic en el enlace con su nombre en la ruta al grupo de administración.
  - La sección **Fijado** del menú principal ahora se llama **Marcadores**. Puede añadir secciones de Kaspersky Security Center Cloud Console a marcadores para acceder a ellas rápidamente.

Actualización de febrero de 2025

Con esta actualización, Kaspersky Security Center Cloud Console se abre y funciona más rápido.

Actualización de octubre de 2024

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes mejoras:

- Hemos mejorado la integración con Microsoft Entra ID. Ahora, cuando un usuario cierra sesión en la cuenta de Microsoft Entra ID que se usó para la autenticación en Kaspersky Security Center Cloud Console, la sesión también termina para Kaspersky Security Center Cloud Console y la sesión del usuario se cierra automáticamente en la consola.

- Ahora puede ver y descargar revisiones de directivas. Kaspersky Security Center Cloud Console le permite ver un informe en formato HTML o guardar la revisión en un archivo JSON.
- Kaspersky Security Center Cloud Console ahora muestra el último estado de la tarea conocido por el Servidor de administración.
- El **Informe sobre ataques de red** ahora incluye la dirección MAC y el puerto del dispositivo atacante.
- Ahora puede cerrar el panel derecho haciendo clic en cualquier lugar fuera del panel. Si realiza algún cambio en el panel y luego intenta cerrarlo haciendo clic fuera del panel, aparecerá una ventana de confirmación.
- El encabezado de la tabla ahora permanece anclado en la parte superior cuando se desplaza por la tabla.

Actualización de septiembre de 2024

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes mejoras:

- Compatible con Kaspersky Endpoint Agent 4.0.
- Varias versiones antiguas de navegadores ya no son compatibles (Chrome anterior a la versión 128, Edge anterior a la versión 128, Firefox ESR anterior a la versión 115, Safari anterior a la versión 17.6).

Actualización de abril de 2024

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Una función nueva de Cloud Discovery. Esta función Cloud Discovery le permite supervisar el uso de servicios en la nube en dispositivos administrados con Windows y bloquear el acceso a los servicios en la nube que considere no deseados. Cloud Discovery rastrea los intentos del usuario de acceder a estos servicios mediante navegadores y aplicaciones de escritorio.
- Integración con Microsoft Entra ID para permitir a los usuarios de su organización iniciar sesión en Kaspersky Security Center Cloud Console con sus credenciales de cuenta de Microsoft Entra ID. Tenga en cuenta que esta función no está disponible en la Federación Rusa.
- Ahora puede crear perfiles de conexión para conectar el Agente de red al Servidor de administración. Los perfiles de conexión permiten que los usuarios de ordenadores portátiles fuera de la oficina cambien el método de conexión a un Servidor de administración o entre Servidores de administración, según la ubicación actual del dispositivo en la red de la empresa.
- Ahora puede abrir la lista de sus espacios de trabajo directamente desde el menú principal de la aplicación.
- Se añadieron dos nuevos idiomas: chino tradicional y chino simplificado.
- La configuración de almacenamiento de eventos predeterminada en la configuración de la tarea se cambió de **Guardar todos los eventos** a **Guardar solo los resultados de ejecución de la tarea**. Esta opción reduce el consumo de espacio en la base de datos del espacio de trabajo. El cambio afecta solo a las tareas creadas para Kaspersky Security Center. Esta configuración permanece sin modificaciones en las tareas para las aplicaciones de seguridad de Kaspersky.
- Kaspersky Security Center Cloud Console ahora también le notifica sobre la eliminación planificada de su espacio de trabajo 7 y 30 días después de que la última clave de licencia se elimine del espacio de trabajo o caduque. Esto le dará más tiempo para comprar otra licencia y añadir su clave de licencia al espacio de trabajo.

- Las infraestructuras de Kaspersky Business Hub y Kaspersky Security Center Cloud Console ahora son compatibles con las licencias de Kaspersky Next. El logotipo de la aplicación se cambia automáticamente de acuerdo con la licencia que utilice.
- Kaspersky Security Center Cloud Console ahora admite las siguientes aplicaciones de Kaspersky:
  - Kaspersky Endpoint Security for Windows, versión 12.4
  - Kaspersky Endpoint Security 12.0 for Mac, parche A
- Cuando migra de una aplicación de seguridad de Kaspersky a otra y la aplicación actual está protegida con contraseña, puede especificar la contraseña de desinstalación directamente en las propiedades de la tarea de instalación remota.
- Ahora puede personalizar el menú principal de la aplicación al anclar o desanclar sus secciones de menú favoritas. Las secciones ancladas se añaden al área **Fijado** para un acceso rápido.
- Interfaz de la aplicación y experiencia del usuario optimizadas cuando selecciona la opción **Al completar otra tarea** mientras programa una tarea.
- El informe sobre el hardware ahora puede incluir información sobre dispositivos macOS.
- Puede seleccionar uno o más dispositivos cliente en la lista de dispositivos y, luego, iniciar una tarea creada previamente para ellos.

Actualización de febrero de 2024

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- En la lista de dispositivos administrados, ahora puede seleccionar un dispositivo o varios dispositivos y, luego, asignar una tarea existente para que se ejecute en los dispositivos seleccionados. El alcance del dispositivo actual de la tarea se reemplazará con los dispositivos que seleccionó.
- Ahora puede asignar etiquetas de dispositivo a varios dispositivos o eliminar etiquetas de dispositivo de varios dispositivos a la vez. En la lista de dispositivos administrados, seleccione los dispositivos y, luego, especifique qué etiquetas desea asignar o eliminar de los dispositivos seleccionados.
- Se optimizaron la apariencia y la experiencia de usuario de la lista de dispositivos administrados. Se añadió una nueva columna **Etiquetas** y la capacidad de filtrar dispositivos por etiquetas de dispositivo.

Actualización de enero de 2024

Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Security 12.4 para Windows.

Actualización de diciembre de 2023

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Ahora, puede verificar la conexión a un sistema SIEM.
- Kaspersky Security Center Cloud Console ahora admite el sondeo de un controlador de dominio de Microsoft Active Directory y un controlador de dominio Samba a través de un punto de distribución basado en Linux.

- Diagnóstico remoto de dispositivos administrados basados en Linux.
- Kaspersky Security Center Cloud Console ahora es compatible con las siguientes aplicaciones de Kaspersky:
  - Kaspersky Endpoint Security para Windows versión 12.3 Parche A
  - Kaspersky Endpoint Security 12.0 para Linux
  - Kaspersky Endpoint Security 12.0 for Mac
  - Kaspersky Endpoint Agent 3.16
  - Kaspersky Embedded Systems Security 3.3 para Windows:
- Se ocultaron dos secciones de la interfaz del menú principal como fuera del alcance de la funcionalidad de la aplicación:
  - Eventos de cifrado (**Operaciones** → **Protección y cifrado de datos** → **Eventos de cifrado**)
  - Rangos IP (**Detección y despliegue** → **Detección** → **Rangos IP**)
- Hemos actualizado el texto del Acuerdo de procesamiento de datos para Kaspersky Security Center Cloud Console.
- Ya no se admiten varias versiones de navegadores antiguos (Firefox ESR anterior a la versión 102).

Actualización de septiembre de 2023

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Embedded Systems Security 3.3 para Linux.
- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Security 12.2 para Windows.
- Optimización de la interfaz de usuario al trabajar con la lista de usuarios en la sección **Activos (dispositivos)**.

Actualización de junio de 2023

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Se publicó una nueva Guía para reforzar la seguridad. Le recomendamos que lea atentamente la guía y siga las recomendaciones de seguridad para configurar Kaspersky Security Center Cloud Console y su infraestructura de red.
- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Security 11.3 for Mac.
- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Security 11.4 para Linux.
- Puede usar Kaspersky Security Center Web Console para exportar selecciones de eventos a un archivo, y luego importar las selecciones de eventos a Kaspersky Security Center Windows o Kaspersky Security Center Linux.

- Ahora puede usar un punto de distribución como servidor push para los dispositivos administrados por el Agente de red. Esta función le permite asegurarse de que se establezca una conectividad continua entre un dispositivo administrado y el Servidor de administración.

- Reorganización de la sección de ajustes para integrar Kaspersky Security Center Cloud Console con otras aplicaciones de Kaspersky.

- Reorganización de la interfaz de usuario de la sección **Diagnósticos remotos**.

- Ahora puede guardar información sobre todos los dispositivos incluidos en una selección de dispositivos en un archivo CSV a la vez.

- Una serie de mejoras en la interfaz de usuario y la usabilidad, incluida la capacidad de seleccionar todos los elementos de una tabla.

Actualización de marzo de 2023

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Kaspersky Security Center Cloud Console ahora admite clústeres y matrices de servidores como dispositivos administrados. Si se instala una aplicación de Kaspersky en un nodo de clúster, el Agente de red envía esta información al Servidor de administración. En Web Console, los clústeres y las matrices de servidores se enumeran aparte de otros dispositivos administrados. Usted administra cada clúster o matriz de servidores como un objeto individual e inseparable.

- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Security 12.0 para Windows.

- La cantidad máxima de entradas que se puede incluir en un informe se incrementó a 2500 para un informe en Web Console y hasta 10 000 para un informe que exporta a un archivo.

- Ahora puede escoger incluir o no los dispositivos administrados con el estado Correcto en el informe de estado de protección.

- Ahora puede activar Kaspersky Security Center Cloud Console mediante una de las siguientes licencias o puede añadir las claves de licencia de las siguientes licencias a un espacio de trabajo existente:

  - Kaspersky Symphony Security

  - Kaspersky Symphony EDR

  - Kaspersky Symphony MDR

  - Kaspersky Symphony XDR

- Se ha lanzado una edición especial de Agente de red para Windows XP.

- El Agente de red actualizado para Linux es compatible con el servicio del Proxy de KSN. Junto con los puntos de distribución basados en Windows, ahora puede usar puntos de distribución basados en Linux para reenviar solicitudes de Kaspersky Security Network (KSN) desde los dispositivos administrados. Esta función le permite redistribuir y optimizar el tráfico en la red.

- El Agente de red actualizado para Linux es compatible con la función de Registro de aplicaciones. El Agente de red puede elaborar una lista de las aplicaciones instaladas en un dispositivo administrado con base en Linux y, luego, transmitir la lista al Servidor de administración.

- Puede usar Kaspersky Security Center Cloud 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.

Actualización de noviembre de 2022

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Security 11.3 para Linux.
- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Managed Endpoint Detection and Response 2.1.18.
- Kaspersky Security Center Cloud Console ahora admite versiones actualizadas de Kaspersky Endpoint Security for Mac 11.2 y 11.2.1, para admitir macOS 13.
- Se actualizaron los vídeos en la sección **Introducción y tutoriales**.

Actualización de octubre de 2022

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Hemos actualizado el texto del Acuerdo de procesamiento de datos para Kaspersky Security Center Cloud Console.
- Ahora, la infraestructura de Kaspersky Security Center Cloud Console le notifica si un espacio de trabajo no tiene una clave de licencia activa y puede eliminarse si no agrega una nueva clave de licencia.
- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Security 11.11.0 para Windows.
- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Detection and Response Optimum 2.3.
- Compatible con Kaspersky Embedded Systems Security 3.2 para Windows.

Actualización de septiembre de 2022

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Ahora puede asignar administradores dedicados para los Servidores de administración virtuales. Cree una cuenta de usuario para un administrador y otorgue al administrador los derechos de acceso a un Servidor de administración virtual. El administrador asignado solo tiene acceso al Servidor de administración virtual seleccionado y no puede conectarse al Servidor de administración principal ni a otros Servidores de administración secundarios, físicos o virtuales.
- Experiencia de usuario optimizada cuando elimina una clave de licencia para Kaspersky Security Center Cloud Console. El nuevo mecanismo evita que elimine su última clave de licencia activa por accidente.
- Ahora puede usar puntos de distribución basados en Linux a fin de descargar bases de datos antivirus para aplicaciones de seguridad de Kaspersky a través de la tarea Descargar actualizaciones en los repositorios de puntos de distribución.

- Ahora el Agente de red está disponible en el idioma de localización japonés.
- En la interfaz de Kaspersky Security Center Cloud Console, se cambió el estilo de las mayúsculas de los nombres de las secciones por el de las mayúsculas de las frases.

Actualización de agosto de 2022

Nuevo idioma compatible: Kaspersky Security Center Cloud Console ahora está disponible en japonés.

Actualización de julio de 2022

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Nuevas versiones de las aplicaciones de Kaspersky compatibles:
  - Kaspersky Endpoint Agent 3.13
  - Kaspersky Endpoint Security 11.2.1 para Mac
  - Kaspersky Security for iOS: 1.0.0
  - Kaspersky Endpoint Security 11.10.0 para Windows
- Hemos actualizado el texto del Contrato y el Acuerdo de procesamiento de datos para Kaspersky Security Center Cloud Console.
- Nuevo idioma compatible: la infraestructura de Kaspersky Security Center Cloud Console ahora está disponible en japonés. La compatibilidad con el idioma japonés dentro de los espacios de trabajo de Kaspersky Security Center Cloud Console llegará pronto.

Actualización de abril de 2022

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Security 11.9.0 para Windows.
- Kaspersky Security Center Cloud Console ahora es compatible con el idioma de localización japonés de Kaspersky Embedded Systems Security.

Actualización de marzo de 2022

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Se implementa la Integración con Kaspersky Endpoint Detection and Response Expert.
- Se implementa la Plataforma de respuesta a incidentes (IRP). Ahora puede administrar los incidentes de seguridad a través de Kaspersky Security Center Cloud Console.
- Kaspersky Security Center Cloud Console ahora acepta claves de licencia para Kaspersky Endpoint Detection and Response Expert. El número mínimo de dispositivos para la licencia es de 50.

Actualización del 11 de febrero de 2022

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Las licencias para Kaspersky Embedded Systems Security para Windows ahora son compatibles.
- Kaspersky Endpoint Security 11.8.0 para Windows es compatible.
- Puede instalar Kaspersky Endpoint Security 11.8.0 para Windows con un paquete de distribución en japonés.
- Compatible con Kaspersky Endpoint Agent 3.12.

Actualización del 10 de diciembre de 2021

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Se ha mejorado el trabajo con usuarios internos:
  - Ahora puede añadir usuarios internos nuevos en el portal.
  - La aplicación ahora evita que disminuya sus propios derechos.

Actualización del 18 de octubre de 2021

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Detection and Response Optimum 2.0.
- Ahora puede administrar dispositivos móviles con Android a través de Kaspersky Security Center Cloud Console.
- Kaspersky Marketplace está disponible como una nueva sección de menú: ahora puede buscar la aplicación de Kaspersky a través de Kaspersky Security Center Cloud Console.
- Una nueva sección del menú, Anuncios de Kaspersky, está disponible. Los anuncios de Kaspersky le mantienen informado mediante información relacionada con las aplicaciones de Kaspersky instaladas en los dispositivos administrados. Kaspersky Security Center Cloud Console actualiza periódicamente la información en la sección.
- Ahora, a través de Kaspersky Security Center Cloud Console, puede administrar Servidores de administración secundarios que ejecuten sistemas operativos Linux.

Actualización del 7 de septiembre de 2021

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Ahora puede usar los Servicios de federación de Active Directory (AD FS) para iniciar sesión en Kaspersky Security Center Cloud Console con su cuenta de Active Directory. Ya no necesitará crear una nueva cuenta de usuario.

- Kaspersky Security Center Cloud Console ahora funciona con los siguientes entornos de nube: Amazon Web Services, Microsoft Azure y Google Cloud. Para proteger máquinas virtuales (o instancias) en un entorno de nube, necesita una de las licencias de Kaspersky Hybrid Cloud Security. El Asistente de configuración del entorno de nube está disponible.

- El número máximo de dispositivos por espacio de trabajo ahora es 25 000.

- La integración con los sistemas SIEM ahora está disponible en Kaspersky Security Center Cloud Console. Ahora puede exportar eventos a sistemas SIEM a través del protocolo Syslog.

- Ahora puede crear Servidores de administración virtuales. Cada Servidor de administración virtual puede tener su propia estructura de grupos de administración, directivas, tareas, informes y eventos. Puede utilizar Servidores de administración virtuales para la gestión de organizaciones cliente con flujos de trabajo complicados dentro de su espacio de trabajo. Sin embargo, no puede migrar Servidores de administración virtuales desde un Kaspersky Security Center que se ejecute en las instalaciones a Kaspersky Security Center Cloud Console.

- Ahora puede ajustar el ancho de las columnas en las tablas, ordenar y buscar datos.

- Hemos mejorado la estabilidad y la disponibilidad de Kaspersky Business Hub y Kaspersky Security Center Cloud Console.

Actualización del 27 de octubre de 2020

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Security 11.6.0 para Windows, Kaspersky Endpoint Security 11.1 for Mac Revisión A y Kaspersky Endpoint Agent 3.10 (como parte de Kaspersky Endpoint Detection and Response Optimum).

- Puede usar las siguientes licencias:

  - Kaspersky Endpoint Detection and Response Optimum

  - Kaspersky Endpoint Security for Business Advanced

  - Kaspersky Total Security for Business

- Están implementadas las siguientes funciones:

  - Administración de vulnerabilidades y parches

  - Administración de cifrado

  - Control de aplicaciones

  - Control de anomalías adaptativo

  - Sesiones de RDP, incluido el Uso compartido del escritorio de Windows

- El menú de navegación ahora es vertical y se asemeja a la interfaz de Kaspersky Security Center basada en Microsoft Management Console.

- Los vídeos de capacitación técnica que ya están disponibles le ayudarán a aprender cómo funciona la aplicación.

Actualización del 30 de junio de 2020

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes características y mejoras:

- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Security 11 for Windows Server (a partir de septiembre de 2020).
- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Agent 3.9 y Kaspersky Endpoint Security 11.4.0 para Windows.
- Se ha mejorado el Asistente de inicio rápido: se han eliminado algunos pasos, la secuencia de pasos ha cambiado ligeramente, se han modificado algunos textos para mejorar su utilidad.
- Kaspersky Security Center Cloud Console ahora está disponible en idioma italiano.
- Ahora puede revocar el Contrato de licencia de usuario final (EULA) de cualquier aplicación de Kaspersky administrada a través de la interfaz de Kaspersky Security Center Cloud Console. Antes de revocar un EULA, deberá desinstalar la aplicación a la que el contrato esté asociado.
- Ahora puede eliminar espacios de trabajo. Si marca un espacio de trabajo para su eliminación, de forma predeterminada se los elimina automáticamente en siete días. Sin embargo, puede forzar la eliminación del espacio de trabajo para que se elimine de inmediato.
- Se ha implementado la verificación en dos pasos para iniciar sesión en la consola.

Kaspersky Security Center Cloud Console

Esta sección incluye información acerca del objetivo de Kaspersky Security Center Cloud Console y de sus características y componentes principales.

Kaspersky Security Center Cloud Console es una aplicación alojada y mantenida por Kaspersky. No es necesario instalar Kaspersky Security Center Cloud Console en su ordenador o servidor. Kaspersky Security Center Cloud Console permite al administrador instalar aplicaciones de seguridad de Kaspersky en dispositivos en una red corporativa, ejecutar tareas de análisis y actualización de forma remota y administrar las directivas de seguridad de las aplicaciones administradas. El administrador puede usar un panel de control detallado que proporciona una instantánea de los estados de los dispositivos corporativos, informes detallados y configuraciones granulares en las directivas de protección.

Acerca de Kaspersky Security Center Cloud Console

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

Kaspersky Security Center Cloud Console le permite hacer lo siguiente:

- Instalar aplicaciones de Kaspersky en dispositivos de su red y administrar aplicaciones instaladas.
- Crear una jerarquía de grupos de administración para administrar una selección de dispositivos cliente como si fueran una sola entidad.
- Crear Servidores de administración virtual y ordenarlos en una jerarquía.
- Proteger sus dispositivos de red, incluidas estaciones de trabajo y servidores:
  - Administre un sistema de protección antimalware creado según las aplicaciones Kaspersky.
  - Use las capacidades de detección y respuesta (EDR y MDR) (se requiere una licencia para Kaspersky Endpoint Detection and Response o para Kaspersky Managed Detection and Response), incluidas las siguientes:
    - Análisis e investigación de incidentes
    - Visualización de incidentes mediante la creación de un gráfico con la cadena de desarrollo de la amenaza
    - Aceptación o rechazo de respuestas de manera manual, o configuración de la aceptación automática de todas las respuestas
- Utilice Kaspersky Security Center Cloud Console como una aplicación de multiinquilinato.
- Gestione de forma remota las aplicaciones de Kaspersky instaladas en dispositivos cliente.
- Realizar un despliegue centralizado de claves de licencia para aplicaciones de Kaspersky en dispositivos cliente.
- Crear y administrar directivas de seguridad para dispositivos en su red.
- Crear y administrar cuentas de usuario.
- Cree y administre funciones de usuario (RBAC).

- Cree y administre tareas para las aplicaciones instaladas en sus dispositivos de red.
- Visualice informes sobre el estado del sistema de seguridad para cada organización cliente de manera individual.

Administra Kaspersky Security Center Cloud Console mediante una Consola de administración basada en la nube que garantiza la interacción entre su dispositivo y el Servidor de administración a través de un navegador. El Servidor de administración es una aplicación diseñada para administrar las aplicaciones Kaspersky instaladas en los dispositivos de red. Cuando se conecta a Kaspersky Security Center Cloud Console con su navegador, el navegador establece una conexión con Servidor de Kaspersky Security Center Cloud Console.

El Servidor de administración y el sistema de administración de bases de datos conectadas (DBMS) se despliegan en un entorno de nube y se le proporcionan como un servicio. El mantenimiento del Servidor de administración y el DBMS se proporciona como parte del servicio. Todos los componentes de software de Kaspersky Security Center Cloud Console se mantienen actualizados. Se hacen copias de seguridad del Servidor de administración y los objetos creados (como directivas y tareas) a intervalos regulares para mantenerlos seguros.

Kaspersky Security Center Cloud Console es una aplicación multilingüe. Puede cambiar el idioma de la interfaz en cualquier momento, sin necesidad de cerrar y volver a abrir la aplicación.

La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antivirus y de la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

Requisitos de hardware y software para Kaspersky Security Center Cloud Console

Consola de administración

Para un cliente, el uso de Kaspersky Security Center Cloud Console solo requiere un navegador:

Puede usar una sola ventana o pestaña del navegador para trabajar con Kaspersky Security Center Cloud Console.

La resolución mínima de pantalla es de 1366x768 píxeles.

Los requisitos de hardware y software del dispositivo son idénticos a los del navegador utilizado para Kaspersky Security Center Cloud Console.

Navegador:

- Google Chrome 133.0.6943.53 o versiones posteriores
- Microsoft Edge 134.0.3124.66 o versiones posteriores
- Safari 17.6 en macOS
- Navegador Yandex 25.2.3.809 o versiones posteriores
- Mozilla Firefox Extended Support Release 128.8.0 o versiones posteriores

Agente de red

Requisitos de hardware mínimos:

- CPU con frecuencia de operación de 1 GHz o superior Para un sistema operativo de 64 bits, la frecuencia de CPU mínima es de 1.4 GHz.
- RAM: 512 MB.
- Espacio disponible en disco: 1 GB.

Requisitos mínimos de hardware para la administración de vulnerabilidades y parches:

- CPU con frecuencia de operación de 1.4 GHz o superior. Se requiere un sistema operativo de 64 bits.
- RAM: 8 GB.
- Espacio disponible en disco: 1 GB.

Sistemas operativos compatibles con el Agente de red

Sistemas operativos. Estaciones de trabajo con Microsoft Windows	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 LTSB (32 bits o 64 bits) Microsoft Windows 10 Enterprise 2016 LTSB (32 bits o 64 bits) Microsoft Windows 10 IoT Enterprise 2015 LTSB (32 bits o 64 bits) Microsoft Windows 10 IoT Enterprise 2016 LTSB (32 bits o 64 bits) Microsoft Windows 10 Enterprise 2019 LTSC (32 bits o 64 bits) Microsoft Windows 10 IoT Enterprise versión 1703, 1709, 1803, 1809 (32 bits o 64 bits) Microsoft Windows 10 20H2, 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 TH1 (julio de 2015) Home/Pro/Pro for Workstations/Enterprise/Education (32/64 bits) Microsoft Windows 10 TH2 (noviembre de 2015) Home/Pro/Pro for Workstations/Enterprise/Education (32/64 bits) Microsoft Windows 10 RS1 (agosto de 2016) Home/Pro/Pro for Workstations/Enterprise/Education (32/64 bits) Microsoft Windows 10 RS2 (abril de 2017) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits/64 bits) Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 RS4 (actualización de abril de 2018, 17134) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 RS5 (octubre de 2018) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 RS6 (mayo de 2019) Home/Pro/Pro for Workstations/Enterprise/Education (32 o 64 bits) Microsoft Windows 10 19H1, 19H2 Home/Pro/Pro for Workstations/Enterprise/Education (32 bit o 64 bit) Microsoft Windows 10 20H1 (actualización de mayo de 2020) Home/Pro/ Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 20H2 (actualización de octubre de 2020) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 21H1 (actualización de mayo de 2021) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits)

	Microsoft Windows 10 21H2 (actualización de octubre de 2021) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 10 22H2 (actualización de octubre de 2023) Home/Pro/Pro for Workstations/Enterprise/Education (32 bits o 64 bits) Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education (64 bits) Microsoft Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education (64 bits) Microsoft Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education (64 bits) Microsoft Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education (64 bits) Microsoft Windows 8.1 Pro/Enterprise (32 bits o 64 bits) Microsoft Windows 8 Pro/Enterprise (32 bits o 64 bits) Microsoft Windows 7 Professional/Enterprise/Ultimate/Home Basic/Premium con Service Pack 1 y versiones posteriores (32 bits o 64 bits) 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)
Sistemas operativos. Servidores de Microsoft Windows	Microsoft Windows MultiPoint Server 2011 Standard/Premium (64 bits) Microsoft Windows Server 2008 Standard/Enterprise/Datacenter/Foundation with Service Pack 2 (32/64 bits) Microsoft Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation con Service Pack 1 y versiones posteriores (64 bits) Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard (64 bits) Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard (64 bits) Microsoft Windows Server 2016 Server Core/Datacenter/Essentials/Standard (opción de instalación) (LTSB) (64 bits) Microsoft Windows Server 2019 Standard/Datacenter/Core (64 bits) Microsoft Windows Server 2019 RS5 Essentials/Standard (64 bits) Microsoft Windows Server 2022 Standard/Datacenter/Core (64 bits) Microsoft Windows Server 2022 21H2 Standard/Datacenter (64 bits) Microsoft Windows Server 2025 Standard/Datacenter/Core (64 bits) Complemento Microsoft Windows Small Business Server 2011 Standard/Essentials/Premium (64 bits)
Sistemas operativos. Linux	Debian GNU/Linux 12 (Bookworm) de 32 bits o 64 bits Debian GNU / Linux 11.x (Bullseye) (32 bits o 64 bits) Ubuntu Server 16.04 LTS (Xenial Xerus) (32 bits o 64 bits) Ubuntu Server 24.04 LTS (64 bits) Ubuntu Server 22.04 LTS (64 bits) Ubuntu Server 20.04 LTS (Focal Fossa) (64 bits) CentOS 7.x (64 bits) CentOS Stream 8 de 64 bits CentOS Stream 9 de 64 bits Red Hat Enterprise Linux Server 9.x (64 bits) Red Hat Enterprise Linux Server 8.x (64 bits) Red Hat Enterprise Linux Server 7.x (64 bits) openSUSE Leap 15 (64 bits) SUSE Linux Enterprise Server 15, todos los Service Pack (64 bits) SUSE Linux Enterprise Server 12, todos los Service Pack (64 bits) Oracle Linux 7 (64 bits) Oracle Linux 8 (64 bits) Oracle Linux 9 (64 bits) Linux Mint 20.x (64 bits) Linux Mint 21.x (64 bits) Linux Mint 22.x (64 bits) Alma Linux 8.x (64 bits) Alma Linux 9.x (64 bits) Rocky Linux 8.x (64 bits)

	Rocky Linux 9.x (64 bits) Amazon Linux 2 (64 bits) Kylin 10 (64 bits)
Sistemas operativos. macOS	macOS Monterey (12.x) macOS Ventura (13.x) macOS Sonoma (14.x) macOS Sequoia (15.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
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x
- Microsoft Hyper-V Server 2019 (64 bits)
- Microsoft Hyper-V Server 2022 (64 bits)
- Máquina virtual basada en kernel (todos los sistemas operativos Linux compatibles con el Agente de red)

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

Aplicaciones y soluciones de Kaspersky compatibles

Las licencias para los diferentes productos otorgan diversos tipos de aplicaciones y soluciones de Kaspersky.

Puede desplegar y administrar las siguientes aplicaciones y soluciones de Kaspersky a través de Kaspersky Security Center Cloud Console:

- Kaspersky Security for Windows Server 11.0.1
- Kaspersky Endpoint Security 12.9 for Windows (solo se admite el cifrado ligero [AES56])
- Kaspersky Endpoint Security 12.2 para Linux
- Kaspersky Endpoint Security 12.1 for Mac
- Kaspersky Embedded Systems Security 3.4 para Windows:
- Kaspersky Embedded Systems Security 3.4 para Linux
- Kaspersky Endpoint Agent 4.0

- Kaspersky Endpoint Security for Android
- Kaspersky Security for iOS

Puede integrar las siguientes soluciones para ver y procesar incidentes de seguridad:

- Kaspersky Managed Detection and Response
- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Endpoint Detection and Response Expert

Si instala una nueva versión de la aplicación en un dispositivo administrado, pero utiliza una directiva desactualizada para la nueva versión de la aplicación en lugar de actualizar la directiva, la aplicación seguirá proporcionando datos a Kaspersky Security Center Cloud Console, pero Kaspersky Security Center Cloud Console no podrá procesar estos datos como se describe en la sección Datos procesados de las aplicaciones administradas de la documentación. Para que Kaspersky Security Center Cloud Console procese estos datos, debe crear una nueva directiva para la nueva versión de la aplicación.

Localización de Kaspersky Security Center Cloud Console

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

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

Comparación de Kaspersky Security Center y Kaspersky Security Center Cloud Console

Puede utilizar Kaspersky Security Center de las siguientes maneras:

- Como solución en la nube

  Kaspersky Security Center se instala para usted en un entorno de nube y Kaspersky le da acceso al Servidor de administración como 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.

- Como una solución local (basada en Windows o basada en Linux)

  Usted instala Kaspersky Security Center en un dispositivo local y administra el sistema de seguridad de la red a través de la Consola de administración para Microsoft Management Console o de Kaspersky Security Center Web Console.

  Además de la aplicación para Windows, también está disponible Kaspersky Security Center Linux. Kaspersky Security Center Linux está diseñado para implementar y administrar la protección de dispositivos Linux mediante el Servidor de administración basado en Linux para cumplir con los requisitos de los entornos Linux puros. Kaspersky Security Center basado en Windows y Kaspersky Security Center Linux tienen diferentes conjuntos de características.

La siguiente tabla le permite comparar las principales funciones de Kaspersky Security Center y Kaspersky Security Center Cloud Console.

Comparación de funciones de Kaspersky Security Center cuando se ejecuta de forma local y cuando lo hace como una solución en la nube

Característica o propiedad	Kaspersky Security Center cuando se ejecuta de forma local	Kaspersky Security Center Cloud Console
Ubicación del Servidor de administración	Local	Nube
Ubicación del sistema de administración de bases de datos (DBMS)	Local	Nube
Consola de administración de nube.	✓	✓
Mantenimiento del Servidor de administración y de la DBMS	Administrado por el cliente	Administrado por Kaspersky
Jerarquía de Servidores de administración	✓	✓ (El Servidor de administración de Kaspersky Security Center Cloud Console solo puede actuar como un Servidor de administración principal en la jerarquía y solo se puede usar para monitorear políticas y tareas)
Jerarquía de grupos de administración	✓	✓
Migración de los dispositivos administrados y objetos asociados desde Kaspersky Security Center local a Kaspersky Security Center Cloud Console	✓	✓
Sondeo de red	✓	✓ (solo por puntos de distribución)
Número de dispositivos administrados	100 000	25 000
Protección de dispositivos administrados: Windows, Linux y macOS	✓	✓
Protección de dispositivos móviles.	✓	✓ (solo se admiten Kaspersky Endpoint Security for Android y Kaspersky Security for iOS)
Protección de infraestructura de nube pública	✓	✓
Administración de la seguridad centrada en el dispositivo	✓	✓
Directivas para aplicaciones	✓	✓
Tareas para aplicaciones de Kaspersky	✓	✓

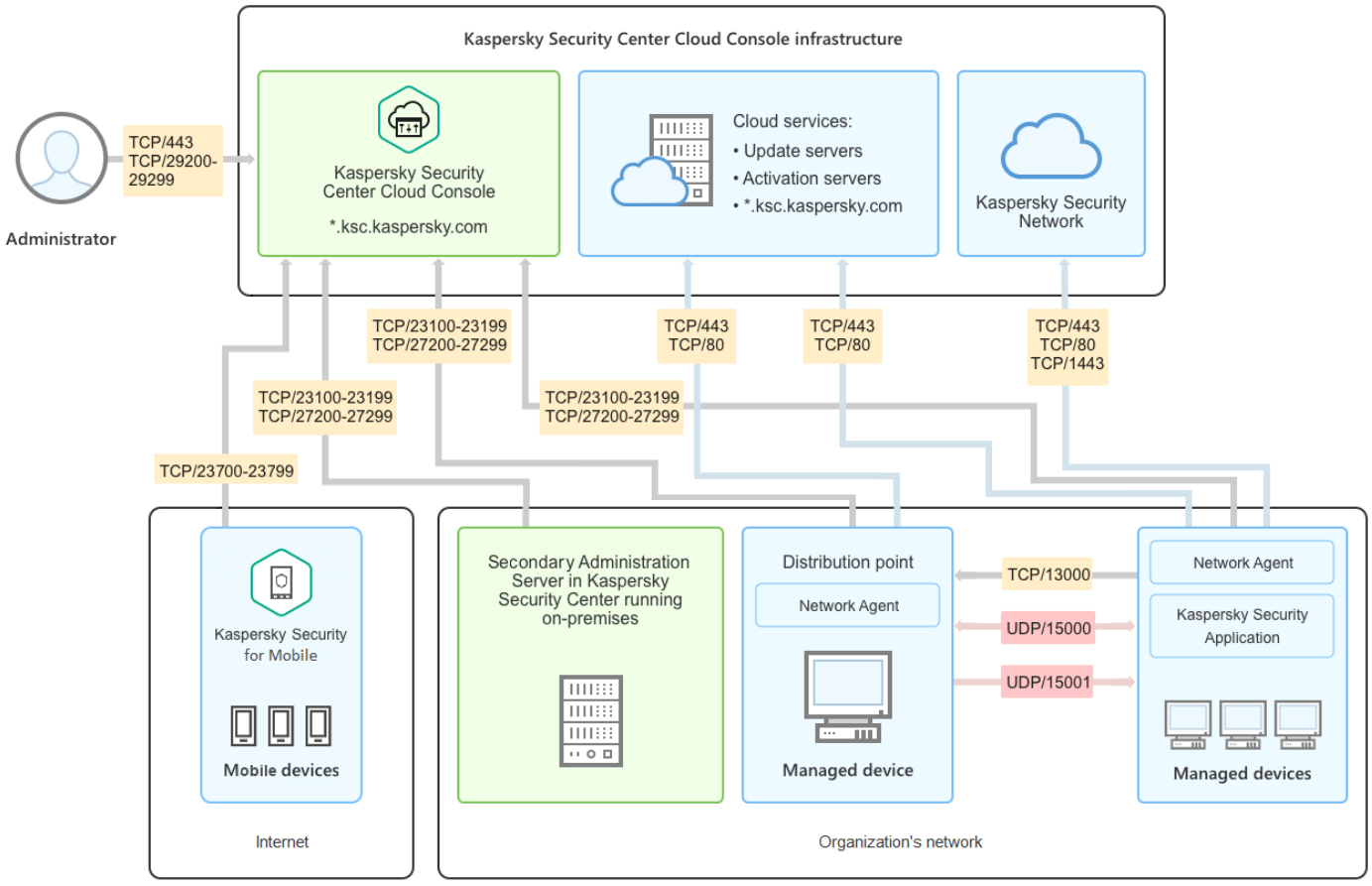
Kaspersky Security Network	✓	✓
Servidor proxy de KSN	✓	✓ (solo en puntos de distribución)
Kaspersky Private Security Network	✓	—
Implementación centralizada de claves de licencia para aplicaciones de Kaspersky	✓	✓
Cambio de dispositivos administrados a otro Servidor de administración	✓	— (debe reinstalar los Agentes de red en los dispositivos administrados para cambiarlos a otro Servidor de administración)
Compatibilidad con servidores de administración virtuales	✓	✓
Instalación de actualizaciones de software de terceros y reparación de vulnerabilidades de software de terceros	✓	✓ (para corregir vulnerabilidades de software de terceros, solo se pueden instalar las correcciones recomendadas)
Notificaciones sobre eventos ocurridos en dispositivos administrados	✓	✓
Creación y gestión de cuentas de usuario	✓	✓
Número máximo de eventos en la base de datos	400 000 (se puede aumentar hasta 45 000 000)	400 000 (depende de la cantidad de dispositivos administrados)
Integración con sistemas SIEM	✓	✓ (solamente mediante el uso del formato Syslog y TLS sobre el protocolo TCP)
Utilizar el Servidor de administración como servidor WSUS	✓	—
Supervisar los estados de políticas y tareas	✓	✓
Compatibilidad con clústeres y conjuntos de servidores en grupos de administración	✓	✓
Instalación remota de sistemas operativos	✓	—
Compatibilidad con SNMP	✓	—
Número máximo de servidores virtuales	500	200
Clonar el disco duro de un dispositivo	✓	—

Arquitectura y conceptos básicos

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

Arquitectura

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



Arquitectura de Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console administrado mediante la consola de nube incluye dos componentes principales: la infraestructura de Kaspersky Security Center Cloud Console y la infraestructura del cliente.

La infraestructura de Kaspersky Security Center Cloud Console está compuesta por los siguientes elementos:

- **Consola de administración de nube**. 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 Cloud Console.
- **Servicios de nube**. Incluye servidores de actualización y servidores de activación.
- **Kaspersky Security Network (KSN)**. Servidores que contienen una base de datos de Kaspersky, que se actualiza continuamente, con información sobre la reputación de los archivos, recursos web y software. Kaspersky Security Network permite que las aplicaciones de Kaspersky respondan más rápidamente a las

amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de encontrarse con falsos positivos.

La infraestructura del cliente puede estar compuesta por los siguientes elementos:

- **Punto de distribución**. Equipo que tiene instalado el Agente de red y se utiliza para la distribución de actualizaciones, el sondeo de la red, la instalación remota de aplicaciones, la recopilación de información sobre equipos en un grupo de administración o dominio de difusión. El administrador selecciona los dispositivos apropiados y les asigna puntos de distribución de forma manual.

- **Dispositivos administrados**. Ordenadores de la red del cliente protegidos mediante Kaspersky Security Center Cloud Console. El Agente de red y una aplicación de seguridad de Kaspersky deben estar instalados en cada dispositivo administrado.

- **Servidor de administración secundario que se ejecuta localmente** (opcional). Puede usar un Servidor de administración local para crear una jerarquía de Servidores de administración.

Puertos utilizados por Kaspersky Security Center Cloud Console

Para utilizar el Kaspersky Security Center Cloud Console, el cual forma parte de la infraestructura de Kaspersky, debe abrir los siguientes puertos en los dispositivos cliente para permitir la conexión a Internet (consulte la siguiente tabla):

Puertos que deben estar abiertos en los dispositivos cliente para permitir la conexión a Internet

Puerto (o rango de puertos)	Protocolo	Propósito del puerto (o rango de puertos)
23100-23199	TCP/TLS	Recepción de conexiones de Agentes de red y Servidores de administración secundarios en el Servidor de administración de Kaspersky Security Center Cloud Console en *.ksc.kaspersky.com. La infraestructura de Kaspersky puede usar cualquier puerto dentro de este rango y cualquier dirección web dentro de esta máscara. El puerto y la dirección web pueden cambiar de vez en cuando.
23700-23799 (solo si administra dispositivos móviles)	TCP/TLS	Recepción de conexiones de dispositivos móviles. Conexión al Servidor de administración de Kaspersky Security Center Cloud Console en *.ksc.kaspersky.com. La infraestructura de Kaspersky puede usar cualquier puerto dentro de este rango y cualquier dirección web dentro de esta máscara. El puerto y la dirección web pueden cambiar de vez en cuando.
27200-27299	TCP/TLS	Recepción de conexiones para la activación de la aplicación de dispositivos administrados (excepto para dispositivos móviles). Conexión al Servidor de administración de Kaspersky Security Center Cloud Console en *.ksc.kaspersky.com. La infraestructura de Kaspersky puede usar cualquier puerto dentro de este rango y cualquier dirección web dentro de esta máscara. El puerto y la dirección web pueden cambiar de vez en cuando.
29200-29299	TCP/TLS	Tunelización de conexiones a dispositivos administrados mediante el uso de la utilidad klsctunnel a través del Servidor de administración de Kaspersky Security Center Cloud Console en *.ksc.kaspersky.com. La infraestructura de Kaspersky puede usar cualquier puerto dentro de este rango y cualquier dirección web dentro de esta máscara. El puerto y la dirección web pueden cambiar de vez en cuando.
443	HTTPS	Conexión al servicio de descubrimiento de Kaspersky Security Center Cloud Console en *.ksc.kaspersky.com. La infraestructura de Kaspersky puede usar cualquier dirección web dentro de esta máscara.
1443	TCP	Conexión a Kaspersky Security Network
80	TCP	La conexión se utiliza para comprobar la validez de los certificados de Kaspersky Security Center en *.digicert.com. La infraestructura de Kaspersky puede usar cualquier dirección web dentro de esta máscara.

La siguiente tabla enumera los puertos que deben estar abiertos en los dispositivos cliente que tengan el Agente de red instalado.

Puertos que deben estar abiertos en los dispositivos cliente

Número de puerto	Protocolo	Objetivo del puerto	Alcance
15000	UDP	Recepción de datos desde las puertas de enlace de conexión (si está en uso)	Administración de dispositivos cliente
15000	Difusión UDP	Obtención de datos sobre otros Agentes de red dentro del mismo dominio de difusión	Entrega de actualizaciones y paquetes de instalación
15001	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

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

También tenga en cuenta que las recomendaciones sobre la compatibilidad de Kaspersky Security Center Cloud Console con software de terceros se describen solo como referencia y es posible que no se apliquen a las nuevas versiones 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 enumera los puertos adicionales que deben estar abiertos en los dispositivos cliente que tengan el Agente de red instalado actuando como un punto de distribución.

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

Número de puerto	Protocolo	Objetivo del puerto	Alcance
13000	TCP/TLS	Recepción de conexiones de los agentes de red	Administración de dispositivos cliente, y entrega de actualizaciones y paquetes de instalación
13111 (solo si el servicio de proxy de KSN se ejecuta en el dispositivo)	TCP	Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN	Servidor proxy de KSN
13295 (solo si utiliza el punto de distribución como servidor push)	TCP/TLS	Envío de notificaciones push a los dispositivos administrados	Punto de distribución utilizado como servidor push
15111 (solo si el servicio de proxy de KSN se ejecuta en el dispositivo)	UDP	Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN	Servidor proxy de KSN
17111 (solo si el servicio de proxy de KSN se ejecuta en el dispositivo)	HTTPS	Recepción de solicitudes enviadas por los dispositivos administrados al servidor proxy de KSN	Servidor proxy de KSN

Si tiene uno o más Servidores de administración en su red y los utiliza como Servidores de administración secundarios cuando el Servidor de administración principal se encuentra en la infraestructura de Kaspersky, consulte la lista de puertos utilizados por Kaspersky Security Center cuando se ejecuta de forma local. Utilice esos puertos para la interacción entre su Servidor de administración secundario (o Servidores de administración secundarios) y los dispositivos cliente.

Conceptos básicos

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

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 Cloud Console. El Agente de red se debe instalar en todos los dispositivos en los que Kaspersky Security Center Cloud Console 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 parámetros:

- Con el nombre "Agente de red de Kaspersky Security Center".
- Se configura de manera que se inicia automáticamente cuando se inicia el sistema operativo.
- Se ejecuta utilizando la cuenta LocalSystem.

Un dispositivo que tiene el Agente de red instalado se denomina *dispositivo administrado* o *dispositivo*. El Agente de red se puede instalar en dispositivos Windows, Linux y Mac.

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

El Agente de red se encarga de sincronizar el dispositivo administrado con el Servidor de administración. Kaspersky Security Center Cloud Console sincroniza automáticamente el Servidor de administración con los dispositivos administrados varias veces por hora. El Servidor de administración establece el intervalo de sincronización (también conocido como el *latido*) en función del número de dispositivos administrados.

Grupos de administración

Un *grupo de administración* (de ahora 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 Cloud Console.

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.

Jerarquía de Servidores de administración

Los Servidores de administración pueden organizarse en una jerarquía de tipo principal/secundario. Cada Servidor de administración puede tener varios Servidores de administración secundarios en distintos niveles de anidamiento de la jerarquía. El nivel de anidamiento para los Servidores de administración secundarios no está limitado. Los grupos de administración del Servidor de administración principal incluirán los dispositivos cliente de todos los Servidores de administración secundarios.

El Servidor de administración de Kaspersky Security Center Cloud Console solo puede actuar como un Servidor de administración principal y solo puede tener como servidores secundarios a Servidores de administración que se ejecuten de forma local.

Al migrar desde el Servidor de administración con ejecución de forma local al Servidor de administración de Kaspersky Security Center Cloud Console, puede organizar los Servidores de administración en forma de jerarquía. Luego, para mitigar la migración, puede cambiar solo una parte de sus dispositivos administrados a la administración del Servidor de administración de Kaspersky Security Center Cloud Console. El resto de los dispositivos administrados permanecen en la administración del Servidor de administración local. Esto le permite probar las funciones de administración de Kaspersky Security Center Cloud Console en un número limitado de dispositivos administrados. Al mismo tiempo, puede configurar directivas, tareas, informes y otros objetos para probar la administración y la supervisión de toda su red. Esto le permite cambiar de nuevo a los objetos configurados en el Servidor de administración local de ser necesario.

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. Para hacerlo, puede usar la función de búsqueda de dispositivos según atributos de red en los grupos de administración de diferentes Servidores de administración.

Servidor de administración virtual

El Servidor de administración virtual (también denominado *servidor virtual*) es un componente de Kaspersky Security Center Cloud Console pensado para administrar protección antivirus de la red de una organización cliente. Cada Servidor de administración virtual puede tener su propia estructura de grupos de administración y sus propios medios de gestión y seguimiento, como directivas, tareas, informes y eventos. El alcance funcional de los Servidores de administración virtuales puede ser utilizado por organizaciones con flujos de trabajo complicados.

El Servidor de administración virtual tiene las siguientes restricciones:

- Los Servidores de administración virtuales son compatibles solo en el modo comercial de Kaspersky Security Center Cloud Console.
- El Servidor de administración virtual no permite la creación de Servidores de administración secundarios (incluidos los Servidores virtuales).
- No se puede migrar servidores de administración virtuales de Kaspersky Security Center a Kaspersky Security Center Cloud Console.
- Los servidores de administración virtuales no pueden ser administrados por administradores dedicados. De forma predeterminada, el administrador que gestiona el Servidor de administración principal también gestiona

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.
- En la ventana de propiedades de Servidor de administración virtual, el número de secciones está restringido.

Punto de distribución

Un *punto de distribución* es un dispositivo con el Agente de red instalado y que se utiliza para la distribución de actualizaciones, la instalación remota de aplicaciones y la extracción de información relativa a dispositivos de red.

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

Un punto de distribución puede realizar las siguientes funciones:

- Distribuir actualizaciones y paquetes de instalación a los dispositivos cliente dentro del grupo (incluida la distribución a través de multidifusión mediante UDP). Las actualizaciones se pueden recibir desde los servidores de actualización de Kaspersky a través de una tarea de actualización creada para el punto de distribución.

  Los puntos de distribución con macOS no pueden descargar actualizaciones de los servidores de actualizaciones de Kaspersky.

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

- Distribuir directivas y tareas de grupo mediante la multidifusión con UDP.
- Actuar como puerta de enlace para la conexión al Servidor de Administración para dispositivos administrados, ya que no se puede establecer una conexión directa en la infraestructura de nube.
- Sondear la red para detectar nuevos dispositivos y actualizar la información disponible sobre los dispositivos de los que ya se tenía conocimiento.
- Realizar la instalación remota de aplicaciones de terceros y Kaspersky a través de las herramientas de Microsoft Windows, incluida la instalación en los dispositivos cliente sin el Agente de red.

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

- Actúa como un servidor proxy que participa en Kaspersky Security Network.

  Esta característica no es compatible con dispositivos de puntos de distribución que ejecuten Linux o macOS.

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

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

A los dispositivos que tengan instalado el Agente de red se les deben asignar puntos de distribución manualmente, según los grupos 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. Sin embargo, el dispositivo que funciona como punto de distribución no puede incluirse en el grupo de administración al cual se lo ha asignado. Cuando existe más de un punto de distribución en la jerarquía de grupos de administración, el Agente de red del dispositivo administrado se conecta con el punto de distribución que más cerca se encuentra en esa jerarquía.

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

Kaspersky Security Center Cloud Console asigna a cada Agente de red una dirección IP de difusión múltiple única que se diferencia del resto de direcciones. Esto le permite evitar que la red se sobrecargue debido a superposiciones de IP.

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

El estado del punto de distribución (*Activo/En espera*) se muestra con una casilla 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 Cloud Console crea un problema de seguridad con el nivel de importancia *Advertencia*. El problema de seguridad se publica en las propiedades del dispositivo, en la sección **Problemas de seguridad**.

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

La ejecución de tareas de actualización (parche) y tareas de reparación de vulnerabilidades en un dispositivo asignado como punto de distribución requiere espacio libre adicional en disco. 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.

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 Cloud 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 Cloud Console y una aplicación específica de Kaspersky. El complemento de administración permite configurar tareas y directivas para esa aplicación.

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
- Funciones de Kaspersky Security Center Cloud Console para mostrar los datos de los sistemas y los eventos de la aplicación y las estadísticas transmitidas desde dispositivos cliente

Directivas

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

Estado de la directiva

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

Las directivas funcionan de acuerdo con las siguientes reglas:

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

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

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

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

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

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

Perfiles de directivas

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

Para ayudarle a evitar la creación de varias instancias de una sola directiva, Kaspersky Security Center Cloud Console 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.

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.

Licencias de la aplicación

En esta sección se proporciona información relacionada con las licencias de la aplicación.

Licencias de Kaspersky Security Center Cloud Console

Después de este escenario, puede comenzar a usar Kaspersky Security Center Cloud Console y las aplicaciones de seguridad administradas con una licencia.

Kaspersky Security Center Cloud Console 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.

Si ya está usando Kaspersky Security Center Cloud Console, puede visitar Kaspersky Marketplace para ver la gama completa de soluciones empresariales de Kaspersky, seleccionar las que necesita y proceder a la compra en el sitio web de Kaspersky.

Revisar las funciones de Kaspersky Security Center Cloud Console en el modo de prueba antes de comprar una licencia

Primero, puede probar Kaspersky Security Center Cloud Console de manera gratuita. Para hacerlo, cree un espacio de trabajo de prueba que finalizará en 30 días. Si desea un espacio de trabajo comercial que pueda usar durante el tiempo que quiera, deberá comprar una licencia.

El modo de prueba no le permite cambiar posteriormente al modo comercial. Cualquier espacio de trabajo de prueba se eliminará automáticamente con todo su contenido cuando caduque su vida útil de 30 días.

Etapas

El escenario avanza en etapas:

1. **Obtener un código de activación para la licencia de Kaspersky Security Center Cloud Console en el modo comercial. Comprar una licencia (o licencias)**

   Las diferentes licencias otorgan el uso de diferentes aplicaciones y servicios de Kaspersky, de modo que puede comprar más de una licencia.

   Descubra las licencias que puede comprar y la cantidad mínima de dispositivos para cada licencia.

   Kaspersky Security Center Cloud Console forma parte de varias soluciones de Kaspersky. Elija la solución que desea usar y compre una licencia para ella. Necesitará comunicarse con Kaspersky o uno de los socios de Kaspersky con una solicitud especial si desea comprar una licencia que cubra 10000 dispositivos o más.

   Utilice la tabla para verificar qué funciones de Administración de vulnerabilidades y parches están disponibles en cada licencia.

   Si desea usar Kaspersky Security Center Cloud Console en un entorno de nube como Microsoft Azure, consulte las opciones de licencia para los entornos de nube.

   Si usted es un Proveedor de servicios gestionados (MSP), consulte las licencias de Kaspersky Security Center Cloud Console para los MSP.

2. **Activación de Kaspersky Security Center Cloud Console durante la creación del espacio de trabajo**

Usted especifica su clave de licencia para activar Kaspersky Security Center Cloud Console cuando crea un espacio de trabajo.

Si tiene más de una clave de licencia, especifique cualquiera de ellas; más adelante deberá añadir otras claves de licencia en Kaspersky Security Center Cloud Console para activar las aplicaciones de Kaspersky administradas.

3. **Añadir claves de licencia para aplicaciones administradas al repositorio del Servidor de administración**

   Antes del despliegue de las claves de licencia, debe añadir estas licencias al repositorio del Servidor de administración.

   La clave de licencia que especificó cuando creó el espacio de trabajo se añade automáticamente al repositorio del Servidor de administración.

   Si tiene más de una clave de licencia, añada sus claves de licencia una por una al repositorio del Servidor de administración de Kaspersky Security Center Cloud Console.

4. **Desplegar claves de licencia para aplicaciones administradas**

   Elija un método de despliegue de la clave de licencia (o claves de licencia) en todos los dispositivos que desea proteger:

   - Despliegue automático

     Si utiliza diferentes aplicaciones administradas y tiene que implementar un código de activación específico para las aplicaciones, elija otra forma de implementar ese código de activación.

     Kaspersky Security Center le permite desplegar automáticamente las claves de licencia disponibles para las aplicaciones administradas. Suponga, por ejemplo, que tiene tres claves de licencia en el repositorio del Servidor de administración. Ha habilitado la opción **Distribuir automáticamente la clave de licencia a los dispositivos administrados** para las tres claves de licencia. Los dispositivos de su organización tienen instalada una aplicación de seguridad de Kaspersky (por ejemplo, Kaspersky Endpoint Security para Windows). Se detecta una nueva aplicación administrada en un dispositivo para la que se debe desplegar una clave de licencia. Por ejemplo, se pueden desplegar dos de las claves de licencia del repositorio para la aplicación administrada en el dispositivo: la clave de licencia llamada *Clave_1* y la clave de licencia llamada *Clave_2*. Una de estas claves de licencia se despliega para la aplicación administrada. En este caso, no se puede predecir cuál de las dos claves de licencia se desplegará porque el despliegue automático de claves de licencia no prevé ninguna actividad de administrador.

     Cuando se despliega una clave de licencia, la cantidad de instalaciones se vuelve a contar para esa clave de licencia. Debe asegurarse de que la cantidad de aplicaciones para las que se ha desplegado la clave de licencia no supere el límite de licencias. Si la cantidad de instalaciones excede el límite de la licencia, se asignará a todos los dispositivos que no estaban cubiertos por la licencia el estado *Crítico*.

     Instrucciones:

     - Agregar una clave de licencia al repositorio del Servidor de administración
     - Distribución automática de una clave de licencia

   - Despliegue con la tarea "Agregar clave de licencia" para una aplicación administrada

     Si opta por usar la tarea Añadir clave de licencia a una aplicación administrada, puede seleccionar la clave de licencia que debe instalarse en los dispositivos y, luego, seleccionar los dispositivos con comodidad, por ejemplo, seleccionando un grupo de administración o una selección de dispositivos.

     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.

5. **Comprobar en qué dispositivos están activadas las aplicaciones administradas de Kaspersky**

   Para asegurarse de que las claves de licencia se desplieguen correctamente, consulte la lista de claves de licencia que se utilizan para una aplicación.

6. **Configurar eventos relacionados con la caducidad de la licencia**

   Configure eventos para recibir una notificación cuando sus claves de licencia se agoten o estén a punto de caducar.

   - Eventos del Servidor de administración: nivel Crítico
   - Eventos del Servidor de administración: nivel Fallo operativo
   - Eventos del Servidor de administración: nivel Advertencia
   - Eventos del Servidor de administración: nivel Información

Acerca del modo de prueba de Kaspersky Security Center Cloud Console

El *Modo de prueba* es un modo especial de Kaspersky Security Center Cloud Console destinado a que el usuario conozca las características de Kaspersky Security Center Cloud Console. En este modo, puede realizar sus actividades dentro de un espacio de trabajo cuyo periodo de validez se limita a 30 días. El modo de prueba se activa automáticamente tan pronto como usted crea un espacio de trabajo de prueba. El conjunto de funciones disponibles en el modo de prueba es idéntico al de la cobertura de la licencia estándar de Kaspersky Endpoint Security for Business Advanced.

En Kaspersky Security Center Cloud Console, no tiene que usar una licencia para el Servidor de administración, porque las funciones que requieren una licencia especial no son compatibles. Si desea utilizar Kaspersky Security Center Cloud Console en el modo de prueba, obtendrá automáticamente una licencia de prueba cuando cree su primer espacio de trabajo.

El modo de prueba no le permite cambiar posteriormente al modo comercial. Cualquier espacio de trabajo de prueba se eliminará automáticamente con todo su contenido cuando caduque su vida útil de 30 días.

Las restricciones siguientes se imponen al uso de las funciones de Kaspersky Security Center Cloud Console en modo de prueba:

- No puede crear una jerarquía de Servidores de administración. No se pueden crear Servidores de administración virtuales.
- La sección de **Licencia** está disponible como solo lectura. Todas las operaciones están prohibidas en esta sección, entre ellas la adición y eliminación de claves de licencia.
- No puede crear paquetes de instalación personalizada.
- No puede crear funciones personalizadas para los usuarios.
- La función Brote de virus no está disponible. Los eventos de brote de virus no se almacenan y no se envían notificaciones.

- El repositorio de **objetos eliminados** no está disponible.
- No puede activar la adición de eventos por lotes (aquellos publicados en grandes cantidades) a la base de datos.
- No se admite la migración de Servidores de administración del modo local al modo de Cloud Console.
- La información estadística de KSN proveniente de los componentes del Servidor de administración, como el Servidor de administración o el Agente de red, no se envía a Kaspersky.

Además, se imponen algunos límites durante la creación de algunos objetos de la aplicación (consulte la siguiente tabla). Si se sobrepasa cualquiera de estos límites cuando se intenta crear dicho objeto, la creación del objeto se bloqueará y se mostrará un mensaje de error sobre el límite.

Limitaciones en la creación de objetos de Kaspersky Security Center Cloud Console en modo de prueba

Tipo de limitación	Valor
Directivas	8
Tareas	17
Claves de licencia	1
Paquetes de instalación	5
Selecciones de dispositivos (instancias preestablecidas no incluidas)	5
Selecciones de eventos (instancias preestablecidas no incluidas)	5
Reglas de movimiento de dispositivos	3
Plantillas de informes del mismo tipo	10
Grupos de seguridad interna	20
Dispositivos administrados	20

Utilizar Kaspersky Marketplace para elegir soluciones empresariales de Kaspersky

Marketplace es una sección del menú principal en la que puede ver el catálogo completo de soluciones empresariales de Kaspersky, seleccionar las soluciones que necesita y adquirir esos productos en el sitio web de Kaspersky. Puede utilizar filtros para ver solo las soluciones que resulten adecuadas para su organización y para los requisitos de su sistema de seguridad de la información. Cuando selecciona una solución, Kaspersky Security Center Cloud Console 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 **Marketplace**:

- Número de dispositivos (endpoints, servidores y otros tipos de activos) que desea proteger:
  - 50–250
  - 250-1000
  - Más de 1000
- Nivel de madurez del equipo de seguridad de la información de su organización:

- **Foundations**

  Este es el nivel típico de las empresas que solo tienen un equipo de TI. Se bloqueará la mayor cantidad de amenazas posible en forma automática.

- **Optimum**

  Este es el nivel típico de las empresas que, dentro de su equipo de TI, tienen personal específicamente a cargo de la seguridad informática. En este nivel, las empresas necesitan soluciones que les permitan contrarrestar tanto amenazas básicas como amenazas que puedan eludir sus mecanismos de prevención existentes.

- **Expert**

  Este es el nivel típico de las empresas que tienen entornos de TI complejos y distribuidos. Estas empresas tienen un equipo de seguridad informática experimentado o un centro de operaciones de seguridad (SOC, 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 **Marketplace**.

   De forma predeterminada, la sección muestra todas las soluciones empresariales de Kaspersky disponibles.

2. Para ver solo aquellas soluciones que sean adecuadas para su organización, seleccione los valores pertinentes en los filtros.

3. Haga clic en la solución que desee comprar o investigar en más detalle.

   Será redirigido a la página web de la solución. Puede seguir las instrucciones en pantalla para proceder con la compra.

Licencias y la cantidad mínima de dispositivos para cada licencia

Si desea utilizar Kaspersky Security Center Cloud Console en modo comercial, tiene que comprar una licencia antes de crear su primer espacio de trabajo. La siguiente tabla muestra las licencias que puede comprar y una cantidad mínima de dispositivos para cada licencia (incluso si desea proteger menos dispositivos):

Licencias que otorgan el uso de Kaspersky Security Center Cloud Console

Licencia	Número mínimo de dispositivos (incluso si desea proteger un número menor)
Kaspersky Endpoint Security for Business Select	Para licencias comerciales: 300 Para licencias comerciales (de suscripción): 100
Kaspersky Endpoint Security for Business Advanced	Para licencias comerciales: 300

	Para licencias comerciales (de suscripción): 100
Kaspersky Total Security for Business	300
Kaspersky Endpoint Detection and Response Optimum	Para licencias comerciales: 300 Para licencias comerciales (de suscripción): 100
Kaspersky Endpoint Detection and Response Expert	50
Kaspersky Hybrid Cloud Security, escritorios	Para licencias comerciales: 300 Para licencias comerciales (de suscripción): 100
Kaspersky Hybrid Cloud Security, servidores	50
Kaspersky Hybrid Cloud Security, núcleos	20
Kaspersky Hybrid Cloud Security, CPU	20
Kaspersky Hybrid Cloud Security Enterprise, equipos de escritorio	Para licencias comerciales: 300 Para licencias comerciales (de suscripción): 100
Kaspersky Hybrid Cloud Security Enterprise, servidores	50
Kaspersky Hybrid Cloud Security Enterprise, CPU	20
Kaspersky Embedded Systems Security	300
Kaspersky Embedded Systems Security Compliance Edition	300
Kaspersky Symphony (por el momento disponible solo en Rusia)	300
Kaspersky Next EDR Foundations	Para licencias comerciales: 300 usuarios Para licencias comerciales (de suscripción): 100 usuarios Cada licencia de usuario se puede aplicar a 1 dispositivo PC/Mac y 2 dispositivos móviles.
Kaspersky Next EDR Optimum	Para licencias comerciales: 300 usuarios Para licencias comerciales (de suscripción): 100 usuarios Cada licencia de usuario se puede aplicar a 1 dispositivo PC/Mac y 2 dispositivos móviles.
Kaspersky Next Complete Security	Para licencias comerciales: 300 usuarios Para licencias comerciales (de suscripción): 100 usuarios Cada licencia de usuario se puede aplicar a 1 dispositivo PC/Mac y 2 dispositivos móviles.
Kaspersky Next EDR Expert	250 usuarios Cada licencia de usuario se puede aplicar a 1 dispositivo PC/Mac y 2 dispositivos móviles.
Kaspersky Next XDR Expert	250 usuarios Cada licencia de usuario se puede aplicar a 1 dispositivo PC/Mac y 2 dispositivos móviles.

Si desea proteger más de 10 000 dispositivos, debe enviar una solicitud al Soporte técnico de Kaspersky y especificar información sobre su empresa y el espacio de trabajo que desea crear.

Eventos sobre límites de licencia superados

Kaspersky Security Center Cloud Console 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 cuando se supera un límite de licencias se define según las siguientes reglas:

- Cuando se ha utilizado entre un 90 % y un 100 % del número total de unidades cubiertas por la licencia, el evento se publica con el nivel de importancia **Información**.
- Cuando se ha utilizado entre un 100 % y un 110 % del número total de unidades cubiertas por la licencia, el evento se publica con el nivel de importancia **Advertencia**.
- Cuando se ha utilizado más de un 110 % del número total de unidades cubiertas por la licencia, el evento se publica con el nivel de importancia **Evento crítico**.

Métodos de distribución de los códigos de activación en los dispositivos administrados

Las aplicaciones de Kaspersky instaladas en los dispositivos administrados se deben licenciar aplicando un código de activación a cada una de las aplicaciones. No puede utilizar archivos de clave para la licencia de aplicaciones administradas: solo se aceptan códigos de activación. Un código de activación se puede desplegar de las siguientes formas:

- Despliegue automático
- La tarea Agregar clave de licencia para una aplicación administrada
- Activar la aplicación administrada manualmente

Las aplicaciones de Kaspersky pueden utilizar más de una clave de licencia al mismo tiempo. Por ejemplo, Kaspersky Endpoint Security para Windows puede utilizar dos claves de licencia: una para Kaspersky Endpoint Security para Windows y otra para la activación de las funciones de Endpoint Detection and Response.

Además, las aplicaciones de Kaspersky pueden tener no solo una clave de licencia activa, sino también una clave de licencia de reserva. 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. Puede agregar una nueva clave de licencia activa o de reserva mediante cualquiera de los métodos enumerados anteriormente. 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.

Añadir una clave de licencia del Servidor de administración

Para añadir una clave de licencia del Servidor de administración:

1. En el menú principal, haga clic en el ícono de configuración ( ) junto al nombre del Servidor de administración.

   La ventana de propiedades del Servidor de administración se abre con la pestaña **General** seleccionada.

2. Vaya a la sección **Claves de licencia** y, a continuación, haga clic en el botón **Seleccionar** en una de las siguientes secciones:

   - **Licencia actual**, si desea añadir una clave de licencia activa.
   - **Clave de licencia de reserva**, si desea añadir una clave de licencia de reserva.

     Puede añadir una clave de licencia de reserva solo si ya se ha añadido una clave de licencia activa.

3. En la ventana que se abre, seleccione una clave de licencia requerida de la tabla.

   Si es necesario, puede añadir una nueva clave de licencia; para ello, haga clic en el botón **Añadir una nueva clave de licencia** y luego introduzca la clave de licencia en el panel derecho que se abre.

4. Haga clic en el botón **Aceptar**.

Se cierra la ventana, se añade la clave de licencia del Servidor de administración y se muestra información sobre la clave de licencia en la sección **Claves de licencia**.

Si es necesario, puede cambiar la clave de licencia seleccionada haciendo clic en el botón **Cambiar** y especificando otra clave de licencia. Además, puede eliminar una clave de licencia.

Agregar una clave de licencia al repositorio del Servidor de administración

Al añadir una clave de licencia mediante Kaspersky Security Center Cloud Console, los parámetros de la clave de licencia se almacenan 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.

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. 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 le permite distribuir una clave de licencia a los dispositivos cliente automáticamente o mediante la tarea **Activación de aplicaciones**. Puede usar la tarea para distribuir claves a un grupo de dispositivos específico. Durante la distribución de una clave de licencia a través de la tarea, no se tiene en cuenta el límite de obtención de licencias en la cantidad de dispositivos. Utilice la distribución automática de claves para detener la distribución de una clave de licencia automáticamente cuando se alcance el límite de licencias.

Si activa la distribución automática de una clave de licencia, no cree una tarea de **Activación de aplicaciones** para distribuir esa clave a los dispositivos cliente. Si lo hace, la carga en el Servidor de administración aumentará debido a la sincronización frecuente.

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 **Activación de aplicaciones**, 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 **Activación de aplicaciones**.
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 **Activación de aplicaciones**.

   - 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, desactive la casilla predeterminada **Usar como clave de reserva** si desea reemplazar la clave de licencia activa.

    Por ejemplo, esto es necesario cuando la organización cambia y se requiere la clave de otra organización en el dispositivo, o si la clave se volvió a emitir y una nueva licencia caduca antes que la licencia actual. Para evitar errores, debe desactivar la casilla **Usar como clave de reserva**.

    Si desea obtener más información sobre los problemas que pueden ocurrir al añadir una clave de licencia a Kaspersky Security Center Windows y las formas de resolverlos, consulte la Base de conocimientos de Kaspersky Security Center.

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 Cloud Console 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, cambie el botón de activación a **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 licencias en la cantidad 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 usted especifica la opción **Distribuir automáticamente la clave de licencia a los dispositivos administrados** para una clave de licencia de suscripción para activar cualquier aplicación en un dispositivo administrado, y al mismo tiempo tiene una clave de licencia de prueba activa, entonces se reemplazará automáticamente su clave de licencia de prueba por la clave de licencia de suscripción ocho días antes de la fecha de caducidad.

Visualizar información acerca de las claves de licencia que están en uso en el repositorio del Servidor de administración

Para ver la lista de las claves de licencia añadidas al repositorio del Servidor de administración,

Vaya a **Operaciones** → **Licencias** → **Licencias de Kaspersky**.

La lista que se muestra contiene los códigos de activación que se añadieron 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.

Visualizar la información acerca de las claves de licencia utilizadas para una aplicación de Kaspersky específica

Para ver las claves de licencia que se están utilizando para una aplicación de Kaspersky:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

   Si el dispositivo pertenece al grupo Dispositivos no asignados, 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, vaya a la sección **Aplicaciones**.

4. En la lista de aplicaciones que se abre, seleccione la aplicación cuyas claves de licencia quiere visualizar.

5. En la ventana de propiedades de la aplicación que se abre, en la pestaña **General**, seleccione la sección **Claves de licencia**.

   La información que busca se mostrará en el espacio de trabajo de la sección.

Eliminación de una clave de licencia del Servidor de administración

Para eliminar una clave de licencia del Servidor de administración:

1. En el menú principal, haga clic en el ícono de configuración ( ) junto al nombre del Servidor de administración.

2. En la ventana de propiedades del Servidor de administración que se abre, seleccione la sección **Claves de licencia**.

3. Haga clic en el botón **Eliminar clave de licencia activa** o **Eliminar clave de licencia de reserva** según la clave de licencia que desee eliminar y, a continuación, en la ventana que se abre, confirme la operación.

Al hacer esto, se elimina la clave de licencia.

Si ha añadido una clave de licencia de reserva, al eliminar la clave de licencia activa, la clave de reserva se convertirá automáticamente en la clave de licencia activa.

Una vez eliminada la clave de licencia activa del Servidor de administración, las funciones Administración de vulnerabilidades y parches y Administración de dispositivos móviles dejan de estar disponibles. Puede volver a añadir una clave de licencia eliminada o añadir una clave de licencia nueva.

Eliminar una clave de licencia del repositorio

Puede eliminar una clave de licencia del repositorio del Servidor de administración. Tenga en cuenta que Kaspersky Security Center Cloud Console elimina automáticamente su espacio de trabajo después de 90 días en los siguientes casos:

- Si usted elimina la última clave de licencia (activa, reservada o no en uso) añadida manualmente en el repositorio.
- Si la última clave de licencia caduca.

Si se elimina su espacio de trabajo, no podrá administrar la protección de su red mediante Kaspersky Security Center Cloud Console. También pierde permanentemente sus datos de Kaspersky Security Center Cloud Console. Si es necesario, puede eliminar su espacio de trabajo manualmente. De lo contrario, le recomendamos que conserve al menos una clave de licencia en el repositorio del Servidor de Administración.

Si elimina una clave de licencia y había añadido una clave de licencia de reserva antes, la clave de licencia de reserva se convierte automáticamente en la clave de licencia activa después de que se elimina la clave activa anterior, o bien si esta caduca.

Cuando elimine la clave de licencia activa desplegada en un dispositivo administrado, la aplicación seguirá funcionando en el dispositivo administrado.

Para eliminar una clave de licencia del repositorio del Servidor de administración, realice lo siguiente:

1. Compruebe que el Servidor de administración no utilice una clave de licencia que desee 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 requerida se muestra 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 no se muestra la clave de licencia necesaria, el Servidor de administración no la utiliza.

2. En el menú principal, vaya a **Operaciones** → **Licencias** → **Licencias de Kaspersky**.

3. Seleccione la clave de licencia necesaria y, a continuación, haga clic en el botón **Eliminar**.

4. En la ventana que aparece, marque la casilla **Entiendo el riesgo y quiero eliminar la clave de licencia**. Esto significa que si elimina la última clave de licencia, está enterado de que se eliminará el espacio de trabajo y perderá el control sobre los dispositivos administrados. Después, haga clic en el botón **Quitar**.

Como resultado, la clave de licencia seleccionada se elimina del repositorio.

Puede volver a añadir una clave de licencia eliminada o añadir otra nueva. Si eliminó la última clave de licencia, también puede añadir una clave de licencia, siempre que todavía no se haya eliminado su espacio de trabajo. Kaspersky Security Center Cloud Console notifica a los administradores del espacio de trabajo 30 días, 7 días y 1 día antes de la eliminación.

Ver la lista de dispositivos donde una aplicación de Kaspersky no está activada

Puede ver la lista de todos los dispositivos donde una aplicación de Kaspersky está instalada, pero no activada (por ejemplo, si falta una licencia o ha caducado).

Para ver los dispositivos donde una aplicación de Kaspersky no está activada:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.

   Se muestra la lista de tareas.

2. Haga clic en el nombre de la tarea Actualizar relacionada con la aplicación de Kaspersky en cuestión.

   Aparece la ventana de propiedades de la tarea. En ella encontrará una serie de pestañas con nombre.

3. En la ventana de propiedades de la tarea, seleccione la sección **Resultados**.

   En la columna **Dispositivo o servidor secundario**, se muestran los dispositivos en los que se realizó correctamente la tarea.

4. Ordene la columna **Dispositivo o servidor secundario**.

   En la columna **Dispositivo o servidor secundario**, se muestran los dispositivos en los que se realizó correctamente la tarea. Los dispositivos donde la tarea falló debido a una licencia faltante son los dispositivos donde la aplicación no está activada.

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. Debe desinstalar la aplicación seleccionada y sus paquetes de instalación antes de revocar su EULA. Es necesario eliminar los paquetes de instalación del Servidor de administración y sus Servidores de administración virtuales.

Los EULA aceptados en un Servidor de administración virtual pueden revocarse en dicho servidor o en el Servidor de administración principal. Los EULA aceptados en un Servidor de administración principal únicamente se pueden revocar en ese mismo Servidor de administración principal.

Para revocar un EULA vinculado a una aplicación de Kaspersky administrada:

1. 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** de las propiedades del Servidor de administración, seleccione la sección **Contratos de licencia de usuario final**.

   Se muestra una lista de los EULA aceptados durante la creación de paquetes de instalación o la instalación sin problemas de actualizaciones.

3. 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.
   - Si el EULA se puede revocar o no.

4. 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.
- Lista de objetos (paquetes de instalación, actualizaciones integradas) vinculados al EULA y sus respectivos nombres y tipos.

5. En la parte izquierda de la ventana de propiedades del EULA, haga clic en el botón **Revocar el Contrato de licencia**.

   Si el EULA seleccionado se puede revocar solo si desinstala la aplicación o si este EULA se puede revocar solo en el Servidor de administración principal, se muestra la notificación sobre esta restricción en lugar del botón **Revocar el Contrato de licencia**.

   > Si existe objetos (paquetes de instalación y sus respectivas tareas) que impiden la revocación del EULA, se muestra la notificación al respecto. 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.

6. 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).

> Si la última clave de licencia caduca, Kaspersky Security Center Cloud Console elimina automáticamente su espacio de trabajo después de 90 días. Como resultado, no podrá administrar la protección de su red mediante Kaspersky Security Center Cloud Console. También pierde permanentemente sus datos de Kaspersky Security Center Cloud Console. Le recomendamos que renueve las claves de licencia obsoletas o añada nuevas claves al repositorio del Servidor de administración para mantener su espacio de trabajo.

Para ver una notificación sobre 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 enlace **Ver licencias por caducar** junto a una notificación.

   Se abre la ventana **Licencias de Kaspersky**, donde puede ver y renovar las licencias que han caducado o están por caducar.

2. Si desea renovar una licencia, haga clic en el enlace **Renovar licencia** junto a la licencia pertinente.

Al hacer clic en un enlace de renovación de licencia, acepta transferir los siguientes datos a Kaspersky: id. del software, versión del software, localización del software, id. de la licencia y un atributo que muestra si la licencia fue proporcionada por una empresa partner. Los datos son necesarios para determinar los términos de renovación de su licencia.

3. Se abrirá una ventana del servicio de renovación de licencias. Siga las instrucciones para renovar la licencia.

   La licencia que estaba por caducar queda renovada.

En Kaspersky Security Center Cloud Console, las notificaciones se muestran cuando una licencia está a punto de caducar, de acuerdo con el siguiente programa:

- 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

Uso de Kaspersky Security Center Cloud Console después de la caducidad de la licencia

Después de caducar la licencia, Kaspersky puede otorgarle el uso de Kaspersky Security Center Cloud Console por hasta 90 días sin limitaciones. Durante este período, el Servidor de administración, el Agente de red y la interfaz web de Kaspersky Security Center Cloud Console funcionan sin limitaciones. Kaspersky Security Center Cloud Console también envía estadísticas de KSN a Kaspersky de acuerdo con la configuración de acceso de KSN vigente. Las aplicaciones administradas trabajan solo con una funcionalidad limitada (para obtener detalles, consulte la documentación de estas aplicaciones).

A los 90 días de haber caducado la licencia, Kaspersky Security Center Cloud Console elimina automáticamente su espacio de trabajo. Si desea mantener el espacio de trabajo, renueve al menos una clave de licencia caducada o añada una nueva al repositorio.

Definiciones de licencia

Esta sección contiene definiciones para los conceptos relacionados con las licencias de aplicaciones de Kaspersky administradas a través de Kaspersky Security Center Cloud Console.

Acerca de la licencia

Una *licencia* otorga el derecho a usar Kaspersky Security Center Cloud Console 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.

  Cuando caduque una licencia de prueba, se desactivarán todas las funciones de Kaspersky Security Center Cloud Console. 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 continuar usando Kaspersky Security Center Cloud Console, debe renovar su 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 vencimiento de la licencia o período 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 añadir una clave de licencia a la aplicación introduciendo un *código de activación*. La clave de licencia se muestra en la interfaz de la aplicación como una secuencia alfanumérica única después de que la agrega a la aplicación.

Kaspersky puede bloquear la clave de licencia en caso de que se hayan infringido los términos del Contrato de licencia. Si la clave de licencia se ha bloqueado, debe agregar otra clave si desea usar la aplicación.

Una clave de licencia puede ser activa o adicional (de reserva).

Una *clave de licencia activa* es la clave que la aplicación está utilizando. Se puede agregar una clave de licencia activa para una licencia de prueba o comercial. La aplicación no puede tener más de una clave de licencia activa.

Una *clave de licencia adicional (o de reserva)* es una clave de licencia que le brinda a una persona el derecho a usar la aplicación, pero que no está activa en un momento dado. Una clave de licencia adicional se activa de forma automática cuando caduca la licencia asociada con la clave de licencia activa actual. Se puede agregar una clave de licencia adicional únicamente si ya se ha agregado una clave de licencia activa.

Se puede agregar una clave de licencia para la licencia de prueba como una clave de licencia activa. No se puede agregar una clave de licencia para la licencia de prueba como una clave de licencia adicional.

Acerca del 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 de licencia que active Kaspersky Security Center Cloud Console. Recibirá el código de activación a través de la dirección de correo electrónico que ha especificado después de adquirir Kaspersky Security Center Cloud Console o tras solicitar la versión de prueba de Kaspersky Security Center Cloud Console.

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 no es posible acceder a los servidores mediante el DNS del sistema, la aplicación utiliza servidores de DNS públicos.

En algunos casos, cuando se ha utilizado un código de activación para activarla, la aplicación se contactará periódicamente con los servidores de activación de Kaspersky a fin de determinar el estado de la clave de licencia. Debe brindarle acceso a Internet a la aplicación para permitir estas comprobaciones.

Si perdió su código de activación después de instalar la aplicación, comuníquese con el socio de Kaspersky a quien le compró la licencia.

Las aplicaciones administradas no se pueden activar utilizando archivos de clave: solo se aceptan códigos de activación.

Acerca de la suscripción

Suscripción a Kaspersky Security Center Cloud Console 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 Cloud Console 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 seguir utilizando Kaspersky Security Center Cloud Console tras la caducidad de una suscripción limitada, debe renovarla. 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 Cloud Console con suscripción, debe aplicar el código de activación facilitado por el proveedor de servicios.

Puede aplicar un código de activación diferente para Kaspersky Security Center Cloud Console solo cuando haya caducado la suscripción o la haya cancelado.

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 mediante suscripción no son válidos para activar versiones anteriores de Kaspersky Security Center Cloud Console.

Al utilizar la aplicación en la modalidad de suscripción, Kaspersky Security Center Cloud Console intenta automáticamente acceder al servidor de activación durante los intervalos de tiempo especificados hasta que caduca 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.

Provisión de datos

Kaspersky Security Center Cloud Console permite al usuario identificar y controlar los dispositivos (y los propietarios de los dispositivos) conectados a Kaspersky Security Center Cloud Console, a través de las funciones de las aplicaciones administradas.

Métodos de provisión de datos:

1. El usuario introduce los datos en la interfaz de Kaspersky Security Center Cloud Console.
2. El Agente de red recibe los datos desde el dispositivo y los transfiere al Servidor de administración.
3. El Agente de red recibe los datos recuperados por la aplicación de Kaspersky administrada y los transfiere al Servidor de administración. La lista de datos que procesan las aplicaciones administradas de Kaspersky se proporciona en la Ayuda de las aplicaciones correspondientes.
4. Los datos se transfieren desde los Servidores de administración secundarios que se ejecutan en las instalaciones.

Kaspersky Security Center Cloud Console elimina automáticamente los espacios de trabajo 30 días después de la caducidad del periodo de vigencia de prueba de la licencia o 90 días después de la caducidad del periodo de vigencia de la licencia comercial.

Una vez que vence el periodo de vigencia de la licencia, Kaspersky guarda los datos del Usuario relacionados con alertas e incidentes en los espacios de trabajo del Usuario durante 30 días.

Con la licencia actual, el plazo de almacenamiento de alertas y de incidencias es de 360 días. Después de este periodo, las alertas y los incidentes más antiguos se eliminan automáticamente.

La eliminación definitiva de los datos enumerados en esta sección puede tardar hasta 24 horas.

Datos que se envían a los servidores de Kaspersky

Datos que se envían durante la activación

Al usar el Código de activación para activar el software, para verificar la legitimidad del uso del software, el usuario acepta proporcionar periódicamente a Kaspersky la siguiente información:

- Código de activación
- Identificador de activación único para la licencia actual

Kaspersky también puede usar esta información para generar información estadística sobre la distribución y el uso del software de Kaspersky.

Datos que se envían durante la actualización

Al recibir las actualizaciones de los servidores de actualizaciones del titular de los derechos, para mejorar la calidad del mecanismo de actualización, el usuario acepta proporcionar periódicamente la siguiente información a Kaspersky:

- Id. de software recibido de la licencia
- Versión completa del software
- Id. de licencia de software
- Id. de instalación de software (PCID)
- Id. del inicio de la actualización de software

Kaspersky también puede usar esta información para generar información estadística sobre la distribución y el uso del software de Kaspersky.

Datos para garantizar un funcionamiento ininterrumpido, un trabajo eficiente y verificar el uso legítimo de Kaspersky Security Center Cloud Console

La siguiente información puede ser utilizada para el propósito especificado:

- Nombres y versiones de las aplicaciones de seguridad de Kaspersky conectadas al espacio de trabajo, así como el número de dispositivos en los que están instaladas estas aplicaciones de seguridad.
- Número de dispositivos con el software de seguridad de Kaspersky instalado que están conectados a todos los espacios de trabajo y distribución de estos dispositivos conectados por tipo.
- Identificador del espacio de trabajo, identificador de la empresa, país y región del espacio de trabajo, y fecha de creación del espacio de trabajo.
- Cantidad de usuarios en el espacio de trabajo, fecha de la última autenticación en el espacio de trabajo.
- Detalles de la licencia utilizada en un momento dado (tipo de licencia, límite de licencia en el número de dispositivos, número de dispositivos conectados y fecha de vencimiento de la licencia antes utilizada).

Datos transferidos cuando se abren los enlaces en la interfaz de Kaspersky Security Center Cloud Console

Al seguir los enlaces de la Consola de administración o de Kaspersky Security Center Cloud Console, el usuario acepta la transferencia automática de los siguientes datos:

- Ubicación de Kaspersky Security Center Cloud Console
- Id. 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.

Datos necesarios para el funcionamiento del espacio de trabajo

Kaspersky Security Center Cloud Console procesa los siguientes datos:

1. Detalles de los dispositivos detectados en la red de la organización

Agente de red recibe los datos que se enumeran a continuación de los dispositivos de la red y los transfiere al Servidor de administración:

a. Especificaciones técnicas del dispositivo detectado y sus componentes requeridos para la identificación del dispositivo que se recibieron mediante el sondeo de la red:

- Sondeo de Active Directory:

  Dispositivos de Active Directory: nombre distintivo del dispositivo; nombre de dominio de Windows recibido del controlador de dominio; nombre del dispositivo en el entorno de Windows; nombre de dominio NetBIOS; dominio DNS y nombre DNS del dispositivo; cuenta del Administrador de cuentas de seguridad (SAM) (nombre de inicio de sesión utilizado para dar soporte a clientes y servidores que ejecutan versiones anteriores del sistema operativo, como Windows NT 4.0, Windows 95, Windows 98 y LAN Manager); nombre distintivo del dominio; nombres distintivos de los grupos a los que pertenece el dispositivo; nombre distintivo del usuario que administra el dispositivo; identificador único global (GUID) y GUID primario del dispositivo.

  Cuando se sondea la red de Active Directory, se procesan los siguientes tipos de datos con el fin de mostrar información sobre la infraestructura administrada y el uso de esta información por parte del usuario, por ejemplo, durante el despliegue de la protección:

- Unidades organizativas de Active Directory: nombre distintivo de la unidad organizativa; nombre distintivo del dominio; GUID y GUID primario de la unidad organizativa.

- Dominios de Active Directory: nombre de dominio de Windows recibido del controlador de dominio; dominio DNS; GUID del dominio.

- Usuarios de Active Directory: nombre para mostrar del usuario; nombre distintivo del usuario; nombre distintivo del dominio; nombre de la organización del usuario; nombre del departamento donde trabaja el usuario; nombre distintivo de otro usuario que actúa como administrador del usuario; nombre completo del usuario; cuenta del Administrador de cuentas de seguridad (SAM); dirección de correo electrónico; dirección de correo electrónico alternativo; número de teléfono principal; número de teléfono alternativo; número de teléfono móvil; nombre del puesto del usuario; nombres distintivos de los grupos a los que pertenece el usuario; identificador único global (GUID) del usuario; identificador de seguridad del usuario (SID) (valor binario único utilizado para identificar al usuario como una entidad de seguridad); nombre principal de usuario (UPN): nombre de inicio de sesión de estilo Internet para un usuario basado en el estándar de Internet RFC 822. El UPN es más corto que el nombre distintivo y más fácil de recordar. Lo habitual es que el UPN se asigne al nombre de correo electrónico del usuario.

- Grupos de Active Directory: nombre distintivo del grupo; dirección de correo electrónico; nombre distintivo del dominio; cuenta del Administrador de cuentas de seguridad (SAM); nombres distintivos de los grupos a los que pertenece el grupo; grupo de id. de seguridad (SID); GUID de grupo.

b. Sondeo del dominio de Samba:

Dispositivos Samba: nombre distinguido del dispositivo; nombre de dominio recibido del controlador de dominio; nombre del dispositivo NetBIOS; nombre de dominio NetBIOS; dominio de DNS y nombre de DNS del dispositivo; cuenta del administrador de cuentas de seguridad (SAM); nombre distinguido del dominio; nombres distinguidos de los grupos a los que pertenece el dispositivo; nombre distinguido del usuario que administra el dispositivo; identificador único global (GUID) y GUID principal del dispositivo.

- Unidades de organización de Samba: nombre distintivo de la unidad organizativa; nombre distintivo del dominio; GUID y GUID primario de la unidad organizativa.

- Dominio de Samba: nombre de dominio de Windows recibido del controlador de dominio; dominio DNS; GUID del dominio.

- Usuarios de Samba: nombre para mostrar del usuario; nombre distintivo del usuario; nombre de la organización del usuario; nombre del departamento donde trabaja el usuario; nombre distintivo de otro usuario que actúa como administrador del usuario; nombre completo del usuario; cuenta del

Administrador de cuentas de seguridad (SAM); dirección de correo electrónico; dirección de correo electrónico alternativo; número de teléfono principal; número de teléfono alternativo; número de teléfono móvil; nombre del puesto del usuario; nombres distintivos de los grupos a los que pertenece el usuario; identificador único global (GUID) del usuario; identificador de seguridad del usuario (SID) (valor binario único utilizado para identificar al usuario como una entidad de seguridad); nombre principal de usuario (UPN): nombre de inicio de sesión de estilo Internet para un usuario basado en el estándar de Internet RFC 822. El UPN es más corto que el nombre distintivo y más fácil de recordar. Lo habitual es que el UPN se asigne al nombre de correo electrónico del usuario.

- Grupos de Samba: nombre distintivo del grupo; dirección de correo electrónico; nombre distintivo del dominio; cuenta del Administrador de cuentas de seguridad (SAM); nombres distintivos de los grupos a los que pertenece el grupo; id. de seguridad (SID) del usuario; GUID de grupo.

c. Sondeo del dominio de Windows:

- Nombre del dominio o grupo de trabajo de Windows
- Nombre NetBIOS del dispositivo
- Dominio DNS y nombre DNS del dispositivo
- Nombre y descripción del dispositivo
- Visibilidad del dispositivo en la red
- Dirección IP del dispositivo
- Tipo de dispositivo (estación de trabajo, servidor, SQL Server, controlador de dominio, etc.)
- Tipo de sistema operativo en el dispositivo
- Versión del sistema operativo del dispositivo
- Hora a la que se actualizó por última vez la información sobre el dispositivo
- Hora a la que el dispositivo estuvo visible por última vez en la red

d. Sondeo de rango IP:

- Dirección IP del dispositivo
- Dispositivo, nombre DNS o nombre NetBIOS
- Nombre y descripción del dispositivo
- Dirección MAC del dispositivo
- Hora a la que el dispositivo estuvo visible por última vez en la red

2. 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 Cloud Console:

a. Especificaciones técnicas y componentes necesarios del dispositivo administrado para su identificación:

- Nombre para mostrar (generado en función del nombre NetBIOS y que se puede modificar manualmente) y descripción del dispositivo (introducido manualmente)
- Nombre y tipo de dominio de Windows (dominio de Windows NT / grupo de trabajo de Windows)
- Nombre del dispositivo en el entorno de Windows
- Dominio DNS y nombre DNS del dispositivo
- Dirección IP del dispositivo
- Máscara de subred del dispositivo
- Ubicación de red del dispositivo
- Dirección MAC del dispositivo
- Número de serie del dispositivo (si está disponible)
- Tipo de sistema operativo en el dispositivo
- Si el dispositivo es una máquina virtual junto con el tipo de hipervisor
- Si el dispositivo es una máquina virtual dinámica como parte de la infraestructura de escritorio virtual (VDI)
- GUID del dispositivo
- Id. de instancia de Agente de red
- Id. de instalación del Agente de red
- Id. permanente del Agente de red

b. Otras especificaciones y componentes de los dispositivos administrados necesarios para su auditoría, así como para tomar decisiones sobre si se aplican actualizaciones y parches específicos:

- Estado de Agente de Windows Update (WUA)
- Arquitectura del sistema operativo
- Proveedor de 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, tipo de máquina virtual
- Tiempo de espera de respuesta del dispositivo
- Si Agente de red se está ejecutando en modo independiente

c. Información detallada sobre la actividad en dispositivos administrados:

- Fecha y hora de la última actualización
- Fecha y hora en la que el dispositivo estuvo visible por última vez en la red
- Reiniciar estado de espera ("Se requiere reiniciar.")
- Hora de encendido del dispositivo

d. Detalles de las cuentas de usuario del dispositivo y sus sesiones de trabajo

e. Estadísticas de funcionamiento si el dispositivo es un punto de distribución:

- Fecha y hora de creación del punto de distribución
- Nombre de la carpeta de trabajo
- Tamaño de la carpeta de trabajo
- Número de sincronizaciones con el Servidor de administración
- Fecha y hora en que el dispositivo se sincronizó por última vez con el Servidor de administración
- Número y tamaño total de los archivos transferidos
- Número y tamaño total de los archivos descargados por clientes
- Volumen de datos descargados por clientes mediante el Protocolo de control de transmisión (TCP)
- Volumen de datos enviados a clientes mediante multidifusión
- Volumen de datos descargados por clientes mediante multidifusión
- Número de distribuciones multidifusión
- Volumen total de distribuciones multidifusión
- Número de sincronizaciones con clientes después de la última sincronización con el Servidor de administración

f. Nombre del Servidor de administración virtual que administra el dispositivo

g. Detalles de los dispositivos de nube:

- Región de la nube
- Nube privada virtual (VPC)
- Zona de disponibilidad en la nube
- Subred de nube
- Grupo de ubicación en la nube

h. Detalles de los dispositivos móviles. La aplicación administrada transfiere estos datos del dispositivo móvil al Servidor de administración. La lista completa de datos está disponible en la documentación de la aplicación administrada.

3. 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:

   a. Componentes de Kaspersky Security Center Cloud Console y aplicaciones de Kaspersky administradas instalados en el dispositivo

   b. Configuración de las aplicaciones de Kaspersky instaladas en el dispositivo administrado:

      - Nombre y versión de la aplicación de Kaspersky
      - Estado
      - Estado de la protección en tiempo real
      - Fecha y hora del último análisis del dispositivo
      - Número de amenazas detectadas
      - Número de objetos que no se pudieron desinfectar
      - Tareas de la aplicación de seguridad de Kaspersky
      - Disponibilidad y estado de los componentes de la aplicación
      - Hora de la última actualización y versión de las bases de datos antivirus
      - Detalles de la configuración de la aplicación de Kaspersky
      - Información sobre las claves de licencia activas
      - Información sobre las claves de licencia adicionales
      - Fecha de instalación de la aplicación
      - Id. de instalación de la aplicación

   c. Estadísticas de funcionamiento de la aplicación: eventos relacionados con los cambios del estado de los componentes de la aplicación de Kaspersky en el dispositivo administrado y con el rendimiento de las tareas iniciadas por los componentes de la aplicación

   d. Estado del dispositivo definido por la aplicación de Kaspersky

   e. Etiquetas asignadas por la aplicación de Kaspersky

   f. Conjunto de actualizaciones instaladas y relevantes para la aplicación de Kaspersky:

      - Nombre para mostrar, versión e idioma de la aplicación
      - Nombre interno de la aplicación
      - Nombre y versión de la aplicación de la clave de registro
      - Carpeta de instalación de la aplicación
      - Versión de parche

- Lista de parches automáticos instalados de la aplicación
- Si la aplicación es compatible con Kaspersky Security Center Cloud Console
- Si la aplicación está instalada en un clúster

g. Detalles de los errores de cifrado de datos en los dispositivos: id. de error, hora de ocurrencia, tipo de operación (cifrado/descifrado), descripción del error, ruta del archivo, descripción de la regla de cifrado, id. del dispositivo y nombre de usuario

4. Eventos de los componentes de Kaspersky Security Center Cloud Console y las aplicaciones administradas de Kaspersky.

   El Agente de red transfiere datos del dispositivo al Servidor de administración.

   La descripción de un evento puede contener los siguientes datos:

   a. Nombre del dispositivo

   b. Nombre de usuario del dispositivo

   c. Nombre del administrador que se ha conectado al dispositivo de forma remota

   d. Nombre, versión y proveedor de la aplicación instalada en el dispositivo

   e. Ruta a la carpeta de instalación de la aplicación en el dispositivo

   f. Nombre de archivo y ruta al archivo en el dispositivo

   g. Nombre de la aplicación y parámetros de la línea de comandos en los que se ejecutó la aplicación

   h. Nombre de parche, nombre del archivo de parche, ID del parche, nivel de la vulnerabilidad corregida por el parche y descripción del error de instalación del parche

   i. Dirección IP del dispositivo

   j. Dirección MAC del dispositivo

   k. Estado de reinicio del dispositivo

   l. Nombre de la tarea que publicó el evento

   m. Si el dispositivo ha cambiado al modo independiente y motivo del cambio

   n. Información sobre el problema de seguridad en el dispositivo: tipo de problema de seguridad, nombre del problema de seguridad, nivel de gravedad, descripción del problema de seguridad, detalles del problema de seguridad transmitidos por la aplicación de Kaspersky

   o. Tamaño del espacio libre en el disco del dispositivo

   p. Si la aplicación de Kaspersky se está ejecutando en modo de funcionalidad limitada, ID de los alcances funcionales

   q. Valores antiguo y nuevo de la configuración de la aplicación de Kaspersky

   r. Descripción del error que se produjo cuando la aplicación de Kaspersky o cualquiera de sus componentes realizaron la operación

5. Configuración de los componentes de Kaspersky Security Center Cloud Console y las aplicaciones administradas de Kaspersky presentadas en las directivas y los perfiles de las directivas.

   El usuario introduce los datos en la interfaz de Kaspersky Security Center Cloud Console.

6. Configuración de las tareas de los componentes de Kaspersky Security Center Cloud Console y las aplicaciones administradas de Kaspersky

   El usuario introduce los datos en la interfaz de Kaspersky Security Center Cloud Console.

7. Datos tratados por la función Administración de vulnerabilidades y parches.

   El Agente de red transfiere los datos que se indican a continuación del dispositivo al Servidor de administración:

   a. Detalles de las aplicaciones y de los parches instalados en los dispositivos administrados (Registro de aplicaciones). Las aplicaciones se pueden identificar de acuerdo con la información sobre los archivos ejecutables detectados en los dispositivos administrados por la función Control de aplicaciones:

      - Id. de aplicación/parche
      - Id. de la aplicación principal (para un parche)
      - Nombre y versión de aplicación/parche
      - Si la aplicación/parche es un archivo .msi de Windows Installer
      - Proveedor de aplicación/parche
      - Id. de idioma de localización
      - Fecha de instalación de aplicación/parche
      - Ruta de instalación de la aplicación
      - Sitio web del servicio de soporte técnico del proveedor de la aplicación/parche
      - Número de teléfono del servicio de soporte técnico
      - Id. de la instancia de aplicación instalada
      - Comentario
      - Clave de desinstalación
      - Clave de instalación en modo silencioso
      - Clasificación de parche
      - Dirección web para obtener información adicional sobre el parche
      - Clave de registro de la aplicación
      - Número de compilación de aplicación
      - SID de usuario
      - Tipo de sistema operativo (Windows, Unix)

b. Información sobre el hardware detectado en los dispositivos administrados (Registro de hardware):

- Id. del dispositivo
- Tipo de dispositivo (placa base, CPU, RAM, dispositivo de almacenamiento masivo, adaptador de vídeo, tarjeta de sonido, controlador de interfaz de red, monitor, dispositivo de disco óptico)
- Nombre del dispositivo
- Descripción
- Proveedor
- Número de serie
- Revisión
- Información sobre el responsable del tratamiento: desarrollador, versión, descripción, fecha de lanzamiento
- Información sobre el BIOS: desarrollador, versión, número de serie, fecha de lanzamiento
- Chipset
- Frecuencia de reloj
- Número de núcleos de CPU
- Número de subprocesos de CPU
- Plataforma de CPU
- Velocidad de rotación del dispositivo de almacenamiento
- RAM: tipo, número de pieza
- Memoria de vídeo
- Códec de tarjeta de sonido

c. Detalles de vulnerabilidades del software de terceros detectadas en los dispositivos administrados:

- Identificador de vulnerabilidad
- Nivel de gravedad de la vulnerabilidad (Advertencia, Alto, Crítico)
- Tipo de vulnerabilidad (Microsoft, de terceros)
- Dirección web de la página en la que se describe la vulnerabilidad
- Hora de creación de la entrada de vulnerabilidad
- Nombre del proveedor
- Nombre localizado del proveedor

- Id. de proveedor
- Nombre de la aplicación
- Nombre localizado de la aplicación
- Código de instalación de la aplicación
- Versión de la aplicación
- Idioma de localización de la aplicación
- Lista de identificadores CVE de la descripción de la vulnerabilidad
- Tecnologías de protección de Kaspersky que bloqueen la vulnerabilidad (Protección frente a amenazas en archivos, Detección de comportamiento, Protección frente a amenazas web, Protección frente a amenazas en el correo, Prevención de intrusiones en el host y ZETA Shield)
- Ruta al archivo de objeto en el que se ha detectado la vulnerabilidad
- Hora de detección de la vulnerabilidad
- ID de los artículos de la Base de conocimientos que figuran en la descripción de la vulnerabilidad
- ID de los boletines de seguridad que figuran en la descripción de la vulnerabilidad
- Lista de actualizaciones en relación con la vulnerabilidad
- Si existe un exploit que aproveche la vulnerabilidad
- Si existe malware que aproveche la vulnerabilidad

d. Detalles de las actualizaciones disponibles para aplicaciones de terceros instaladas en dispositivos administrados:

- Nombre de aplicación y versión
- Proveedor
- Idioma de localización de la aplicación
- Sistema operativo
- Lista de parches según la secuencia de instalación
- Versión original de la aplicación a la que se aplica el parche
- Versión de aplicación tras la instalación del parche
- ID de parche
- Número de compilación
- Indicadores de instalación
- Contratos de licencia para el parche

- Si el parche es un requisito previo para la instalación de otros parches
- Lista de las aplicaciones instaladas requeridas y sus actualizaciones
- Fuentes de información sobre el parche
- Información adicional sobre el parche (direcciones de páginas web)
- Dirección web para descargar parches, nombre de archivo, versión, revisión y SHA256

e. Detalles de las actualizaciones de Microsoft encontradas por la función WSUS:

- Número de revisión de la actualización
- Tipo de actualización de Microsoft (controlador, software, categoría, detectoid)
- Nivel de importancia de la actualización de acuerdo con el boletín del Centro de respuesta de seguridad de Microsoft (MSRC) (bajo, medio, alto, crítico)
- Id. de los boletines del MSRC relacionados con la actualización
- Id. de los artículos en la Base de conocimientos del MSRC
- Nombre de la actualización (encabezado)
- Descripción de la actualización
- Si el instalador de actualizaciones es interactivo
- Indicadores de instalación
- Clasificación de actualización (actualizaciones críticas, actualizaciones de definiciones, controladores, paquetes de funciones, actualizaciones de seguridad, Service Packs, herramientas, paquetes acumulativos de revisiones, actualizaciones y cambio de versión)
- Información sobre la aplicación a la que se aplica la actualización
- ID de Contrato de licencia de usuario final (EULA)
- Texto EULA
- Si el EULA debe aceptarse para la instalación de la actualización
- Información sobre las actualizaciones asociadas (ID y número de revisión)
- ID de actualización (identidad de actualización global de Microsoft Windows)
- ID de actualizaciones reemplazadas
- Si la actualización está oculta
- Si la actualización es obligatoria
- Estado de instalación de actualización (no aplicable, no asignada para instalación, asignada, instalando, instalada, fallida, requiere reiniciar y no asignada para instalación (nueva versión))

- ID de CVE de la actualización
- Empresa que publicó la actualización o valor "Falta la empresa"

f. Lista de las actualizaciones de Microsoft encontradas por la función WSUS que se deben instalar en el dispositivo.

8. Información sobre los archivos ejecutables detectados en los dispositivos administrados por la función Control de aplicaciones (puede estar asociada a la información del Registro de aplicaciones). Se proporciona una lista completa de detalles en la sección que describe los datos de los dispositivos administrados a través de la aplicación correspondiente.

   La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red.

9. Información sobre los archivos colocados en Depósito de copias de seguridad. Se proporciona una lista completa de detalles en la sección que describe los datos de los dispositivos administrados a través de la aplicación correspondiente.

   La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red.

10. Información sobre los archivos solicitados por los expertos de Kaspersky para un análisis detallado. Se proporciona una lista completa de detalles en la sección que describe los datos de los dispositivos administrados a través de la aplicación correspondiente.

    La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red.

11. Información sobre el estado y la activación de las reglas de control de anomalías adaptativo. Se proporciona una lista completa de detalles en la sección que describe los datos de los dispositivos administrados a través de la aplicación correspondiente.

    La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red.

12. Información sobre los dispositivos (unidades de memoria, herramientas de transferencia de información, herramientas de impresión de información y buses de conexión) instalados o conectados al dispositivo administrado y detectados por la función Control de dispositivos. Se proporciona una lista completa de detalles en la sección que describe los datos de los dispositivos administrados a través de la aplicación correspondiente.

    La aplicación administrada transfiere datos del dispositivo al Servidor de administración a través del Agente de red.

13. Datos sobre alertas:

    - Fecha y hora del primer evento de telemetría en la alerta
    - Fecha y hora del último evento de telemetría en la alerta
    - Nombre de la regla activada (el usuario introduce esto en la interfaz de Kaspersky Security Center Cloud Console)
    - Estado de alerta
    - Resolución (falso positivo, verdadero positivo, prioridad baja)
    - ID y nombre del usuario que está asignado para la alerta

- ID único en la base de datos de Kaspersky Security Center Cloud Console y el nombre del dispositivo relacionado con los eventos que son fuentes de alerta
- SID y nombre de usuario del dispositivo relacionado con los eventos que son fuentes de alerta
- Observables, es decir, datos observables relacionados con los eventos que son fuentes de alerta:
  - Dirección IP
  - Suma del hash MD5 del archivo y de la ruta del archivo
  - Dirección web
  - De dominio
- Detalles adicionales del objeto relacionado con la alerta (recibidos de la aplicación)
- Comentarios a la alerta:
  - Fecha y hora en que se añadió el comentario
  - Usuario que añadió el comentario
  - Texto del comentario
- Alerta de registro de cambios:
  - Fecha y hora del cambio
  - Usuario que realizó el cambio
  - Descripción del cambio

14. Datos sobre problemas de seguridad:

- Fecha y hora del primer evento en el problema de seguridad
- Fecha y hora del último evento en el problema de seguridad
- Nombre del problema de seguridad (el usuario lo introduce en la interfaz de Kaspersky Security Center Cloud Console)
- Breve descripción del problema de seguridad
- Prioridad del problema de seguridad
- Estado del problema de seguridad
- ID y nombre del usuario asignado para el problema de seguridad
- Resolución (falso positivo, verdadero positivo, baja prioridad, fusionado)
- Comentario del problema de seguridad:
  - Fecha y hora en que se añadió el comentario

- Usuario que añadió el comentario
- Texto del comentario

- Registro de cambios de problemas de seguridad:
  - Fecha y hora del cambio
  - Usuario que realizó el cambio
  - Descripción del cambio

15. Datos tratados por la función de cifrado de datos de las aplicaciones de Kaspersky.

    La aplicación administrada transfiere los datos que se indican a continuación desde el dispositivo al Servidor de administración a través de Agente de red. El usuario introduce la descripción de la unidad en la interfaz de Kaspersky Security Center Cloud Console:

    a. Lista de las unidades en los dispositivos:
       - Nombre de la unidad
       - Estado de cifrado
       - Tipo de unidad (de arranque, de disco)
       - Número de serie de la unidad
       - Descripción

    b. Detalles de los errores de cifrado de datos en los dispositivos:
       - Fecha y hora en que ocurrió el error
       - Tipo de operación (cifrado, descifrado)
       - Descripción del error
       - Ruta del archivo
       - Descripción de la regla
       - Id. del dispositivo
       - Nombre de usuario
       - ID del error

    c. Configuración de cifrado de datos de la aplicación Kaspersky.

       Se proporciona una lista completa de detalles en la sección que describe los datos de los dispositivos administrados a través de la aplicación correspondiente.

16. Detalles de los códigos de activación introducidos.

    El usuario introduce los datos en la interfaz de Kaspersky Security Center Cloud Console.

17. Cuentas de usuario.

El Usuario introduce los datos que se indican a continuación en la interfaz de Kaspersky Security Center Cloud Console:

a. Nombre

b. Descripción

c. Nombre completo

d. Dirección de correo electrónico

e. Número de teléfono principal

f. Contraseña

g. Código de seguridad de un solo uso para la verificación en dos pasos

18. Datos necesarios para la autenticación de usuarios mediante Active Directory:

    a. Configuración de los Servicios de federación de Active Directory (AD FS):

    - URL principal del proveedor de autenticación
    - Certificados raíz de confianza para AD FS
    - Id. de cliente generado en AD FS
    - Clave secreta para proteger el acceso a AD FS
    - Alcance de los tokens
    - Dominio de Active Directory con el que se realiza la integración
    - Nombre del campo del token que contiene el SID del usuario
    - Nombre del campo de token que contiene la matriz de SID de los grupos de usuarios

    El usuario introduce los datos en la interfaz de Kaspersky Security Center Cloud Console.

19. Datos necesarios para autenticar a los usuarios mediante Microsoft Entra ID.

    a. Configuración de la integración con Microsoft Entra ID:

    - Id. del inquilino de Microsoft Entra ID
    - Id. de cliente generado en el inquilino de Microsoft Entra ID
    - Secreto de cliente creado en el inquilino de Microsoft Entra ID

    El usuario introduce los datos en la interfaz de Kaspersky Security Center Cloud Console.

    a. Datos sobre usuarios y grupos en el inquilino de Microsoft Entra ID, que Kaspersky Security Center Cloud Console recibe como resultado del sondeo de Microsoft Entra ID:

    - Datos sobre usuarios en el inquilino de Microsoft Entra ID: identificador de objeto de usuario; identificador de seguridad del usuario; nombre para mostrar del usuario; nombre de la organización del

usuario; nombre del departamento en el que trabaja el usuario; puesto del usuario; dirección de correo electrónico; número de teléfono principal; número de teléfono móvil; nombre de usuario; nombres de los grupos a los que pertenece el usuario.

- Datos sobre usuarios creados en Microsoft Entra ID como resultado de la sincronización con Active Directory local: identificador de seguridad del usuario en Active Directory local; nombre de dominio en Active Directory local; nombre de usuario en Active Directory local; cuenta SAM del usuario en Active Directory local; nombre de usuario distinguido en Active Directory local.

- Datos sobre grupos en el inquilino de Microsoft Entra ID: identificador de objeto de grupo; identificador de seguridad de grupo; nombre para mostrar del grupo; dirección de correo electrónico; nombres de otros grupos a los que pertenece el grupo.

- Datos sobre grupos creados en Microsoft Entra ID como resultado de la sincronización con Active Directory local: identificador de seguridad del grupo en Active Directory local; cuenta SAM del grupo en Active Directory local.

20. Historial de revisión de objetos de administración: Servidor de administración, Grupo de administración, Directiva, Tarea, Usuario / grupo de seguridad, Paquete de instalación.

    a. El Usuario introduce los datos que se indican a continuación en la interfaz de Kaspersky Security Center Cloud Console:

    - Servidor de administración

    - Grupo de administración

    - Directiva

    - Tarea

    - Usuario/grupo de seguridad

    - Paquete de instalación

    b. Dirección IP del dispositivo en el que el usuario creó una revisión. El Servidor de administración detecta la dirección IP automáticamente.

21. Registro de objetos de administración eliminados.

    El usuario introduce los datos en la interfaz de Kaspersky Security Center Cloud Console.

22. Paquetes de instalación creados a partir del archivo y ajustes de instalación.

    El usuario introduce los datos en la interfaz de Kaspersky Security Center Cloud Console.

23. Datos necesarios para mostrar los anuncios de Kaspersky en Kaspersky Security Center Cloud Console:

    a. Información sobre las aplicaciones de Kaspersky administradas utilizadas por el Usuario: Id. de la aplicación, número de versión completa.

    b. La ubicación del Usuario de la interfaz de Kaspersky Security Center Cloud Console.

    c. Información sobre la activación del Software en el Dispositivo: Id. de licencia del Software; periodo de vigencia de la licencia del Software; fecha y hora de caducidad de la licencia del Software; tipo de licencia de Software utilizada; tipo de suscripción de Software; fecha y hora de caducidad de la suscripción del Software; estado actual de la suscripción del Software; motivo del estado actual/cambio de estado de la

suscripción del Software; Id. del artículo de la lista de precios a través del cual se adquirió la licencia del Software.

d. Información sobre el acuerdo legal aceptado por el Usuario mientras usa el Software: tipo de acuerdo legal; versión del acuerdo legal; marcador que indica si el usuario ha aceptado las condiciones del acuerdo legal.

e. Información sobre los anuncios recibidos del Titular de los derechos: Id. de anuncio; hora de recepción del anuncio; estado de recepción del anuncio.

El usuario introduce los datos en la interfaz de Kaspersky Security Center Cloud Console.

24. Configuración de usuario de Kaspersky Security Center Cloud Console.

    El Usuario introduce los datos que se indican a continuación en la interfaz de Kaspersky Security Center Cloud Console:

    a. Idioma de localización de la interfaz de usuario

    b. Tema de la interfaz de usuario

    c. Configuración de visualización del panel de supervisión

    d. Información sobre el estado de las notificaciones: ya leída/aún no leída

    e. Estado de las columnas de las hojas de cálculo: mostrar/ocultar

    f. Progreso del tutorial

25. Datos recibidos al usar la función de diagnóstico remoto en un dispositivo administrado: archivos de seguimiento, información del sistema, detalles de las aplicaciones de Kaspersky instaladas en el dispositivo, archivos de volcado, archivos de registros, resultados de la ejecución de los scripts de diagnóstico recibidos del Servicio de soporte técnico.

26. Datos que el Usuario introduce en la interfaz de Kaspersky Security Center Cloud Console:

    a. Nombre del grupo de administración al crear una jerarquía de grupos de administración

    b. Dirección de correo electrónico al configurar las notificaciones de correo electrónico

    c. Etiquetas para dispositivos y reglas de etiquetado

    d. Etiquetas para aplicaciones

    e. Categorías de usuario de las aplicaciones

    f. Nombre de la responsabilidad asignada a un usuario

    g. Información sobre subredes: nombre, descripción, dirección y máscara de subred

    h. Configuración de informes y selecciones

    i. Cualquier otro dato introducido por el Usuario

27. Datos recibidos de un Servidor de administración secundario implementado en las instalaciones.

    Los datos procesados por el Servidor de administración de Kaspersky Security Center se describen en la Ayuda en línea de Kaspersky Security Center.

Al conectar un servidor de administración de Kaspersky Security Center Cloud Console implementado en las instalaciones como secundario en relación con Kaspersky Security Center Cloud Console, esta procesa los siguientes tipos de datos del servidor de administración secundario:

a. Información sobre los dispositivos de la red de la empresa, recibida como resultado de la detección de dispositivos en la red de Active Directory o en la red de Windows, o mediante el análisis de intervalos IP

b. Información sobre las unidades organizativas, los dominios, los usuarios y los grupos de Active Directory, recibida como resultado del sondeo de red de Active Directory

c. Información sobre los dispositivos administrados, sus especificaciones técnicas (incluidas las necesarias para la identificación de dispositivos), las cuentas de los usuarios de dispositivo y sus sesiones de trabajo

d. Información sobre los dispositivos móviles, transferida mediante el protocolo Exchange ActiveSync

e. Información sobre los dispositivos móviles, transferida mediante el protocolo MDM de iOS

f. Detalles de las aplicaciones de Kaspersky instaladas en el dispositivo: configuración, estadísticas de funcionamiento, estado del dispositivo definido por la aplicación, actualizaciones instaladas y aplicables, y etiquetas

g. Información transferida con la configuración de eventos de los componentes de Kaspersky Security Center y las aplicaciones administradas de Kaspersky

h. Configuración de los componentes de Kaspersky Security Center y las aplicaciones administradas de Kaspersky presentadas en las directivas y los perfiles de las directivas

i. Configuración de las tareas de los componentes de Kaspersky Security Center y las aplicaciones administradas de Kaspersky

j. Datos tratados por la función Administración de vulnerabilidades y parches: detalles de aplicaciones y parches; información sobre el hardware; detalles de vulnerabilidades del software de terceros detectadas en los dispositivos administrados; detalles de actualizaciones disponibles para aplicaciones de terceros; y detalles de las actualizaciones de Microsoft encontradas por la función WSUS

k. Categorías de usuario de las aplicaciones

l. Detalles de los archivos ejecutables detectados en los dispositivos administrados por la función Control de aplicaciones

m. Detalles de los archivos colocados en Depósito de copias de seguridad

n. Detalles de los archivos puestos en Cuarentena

o. Detalles de los archivos solicitados por los expertos de Kaspersky para un análisis detallado

p. Información sobre el estado y el desencadenamiento de las reglas de control de anomalías adaptativo

q. Detalles de los dispositivos (unidades de memoria, herramientas de transferencia de información, herramientas de impresión de información y buses de conexión) instalados o conectados al dispositivo administrado y detectados por la función Control de aplicaciones

r. Configuración de cifrado de la aplicación de Kaspersky: repositorio de claves de cifrado, estado de cifrado del dispositivo

s. Información sobre los errores de cifrado de datos generados en los dispositivos al usar la función de cifrado de datos de las aplicaciones de Kaspersky

t. Lista de controladores lógicos programables (PLC) administrados

u. Detalles de los códigos de activación introducidos

v. Cuentas de usuario

w. Historial de revisiones de los objetos de administración

x. Registro de objetos de administración eliminados

y. Paquetes de instalación creados a partir del archivo, así como configuración de instalación

z. Configuración de usuario de Kaspersky Security Center Web Console

aa. Cualquier dato que el usuario introduce en la interfaz de la Consola de administración o la Kaspersky Security Center Cloud Console

ab. Certificado para la conexión segura de dispositivos administrados a los componentes de Kaspersky Security Center

28. Información cargada desde el dispositivo administrado al utilizar la función de diagnóstico remoto: archivos de diagnóstico (archivos de volcado, archivos de registro, archivos de seguimiento, etc.) y los datos que contengan dichos archivos.

29. Datos necesarios para la integración de Kaspersky Security Center Cloud Console con un sistema SIEM para la exportación de eventos:

- Datos necesarios para la conexión y la autenticación:
  - Dirección y puerto de conexión del sistema SIEM
  - Certificado de autenticación del servidor SIEM
  - Certificado de confianza y clave privada para la autenticación del cliente de Kaspersky Security Center Cloud Console en el sistema SIEM

  El usuario introduce los datos en la interfaz de Kaspersky Security Center Cloud Console.

- Datos que Kaspersky Security Center Cloud Console recibe del sistema SIEM: clave pública del certificado del servidor SIEM para la autenticación del servidor SIEM.

30. Datos necesarios para la interacción de Kaspersky Security Center Cloud Console con el entorno de nube:

a. Amazon Web Services (AWS):

- Id. de la clave de acceso de la cuenta de usuario de IAM
- Clave secreta de la cuenta de usuario de IAM

b. Microsoft Azure:

- Id. de la aplicación en Azure
- Id. de suscripción de Azure
- Contraseña de la aplicación en Azure

- Nombre de cuenta para el repositorio de Azure
- Clave de acceso a la cuenta para el repositorio de Azure

c. Google Cloud:

- Correo electrónico del cliente de Google
- Id. de proyecto
- Clave privada

El usuario introduce los datos en la interfaz de Kaspersky Security Center Cloud Console.

31. Datos transferidos por una aplicación de Kaspersky no compatible.

    Cuando instala el Agente de red en un dispositivo que tiene instalada una aplicación de Kaspersky que no es compatible con Kaspersky Security Center Cloud Console, esta aplicación de Kaspersky seguirá transfiriendo los datos a Kaspersky Security Center Cloud Console (hay una lista de los datos disponible en la sección "Sobre la provisión de datos" en el sistema de ayuda de la aplicación). Sin embargo, Kaspersky Security Center Cloud Console no podrá procesar los datos que transfiera la aplicación incompatible tal como se describe para la funcionalidad principal de Kaspersky Security Center Cloud Console.

    La lista de aplicaciones de Kaspersky compatibles se puede consultar en la Ayuda en línea de Kaspersky Security Center Cloud Console.

32. Información estadística sobre los intentos del usuario de obtener acceso a los servicios en la nube.

    Una aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Para obtener la lista completa de datos transferidos, consulte la Ayuda de la aplicación administrada.

33. Datos para crear una cadena de desarrollo de amenazas.

    Una aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Para obtener la lista completa de datos transferidos, consulte la Ayuda de la aplicación administrada.

34. Datos necesarios para la integración de Kaspersky Security Center con el servicio Kaspersky Managed Detection and Response.

    Token para el inicio de la integración, token de integración y token de sesión del usuario. El usuario introduce el token para iniciar la integración en la interfaz de Kaspersky Security Center Cloud Console. El servicio de Kaspersky Managed Detection and Response transfiere tanto el token de integración como el token de sesión del usuario a través del complemento MDR.

Datos necesarios para el funcionamiento de las aplicaciones administradas

Las siguientes aplicaciones administradas transfieren datos desde el dispositivo al Servidor de administración a través del Agente de red:

- Kaspersky Endpoint Security para Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Agent

- Kaspersky Security for Windows Server
- Kaspersky Security for Mobile
- Kaspersky Embedded Systems Security para Windows
- Kaspersky Embedded Systems Security para Linux

La lista de datos procesados se encuentra publicada en https://ksc.kaspersky.com/Home/LegalDocuments, en el Acuerdo de procesamiento de datos de Kaspersky Security Center Cloud Console. En la página web de documentos legales, busque el bloque de texto llamado Contrato de Kaspersky Security Center Cloud Console luego desplácese hacia abajo en el bloque de texto hasta Datos para dispositivos administrados a través de la aplicación administrada correspondiente. También puede utilizar la función de búsqueda estándar de su navegador con el mismo propósito.

Datos de usuario procesados de forma local

El único componente de Kaspersky Security Center que se puede implementar de forma local en Kaspersky Security Center Cloud Console es el Agente de red.

Lista de datos de usuario procesada de forma local:

- Todos los datos enumerados en la sección Datos del usuario procesados dentro del marco y la infraestructura de Kaspersky, excepto los datos que el administrador ingresa a través de la interfaz de Kaspersky Security Center Cloud Console
- Registro de eventos de Kaspersky del Agente de red
- Las trazas del Agente de red
- Registros, incluidos los registros creados por el instalador del Agente de red, las utilidades de Kaspersky Security Center

Los archivos de volcado, registro y seguimiento de Agente de red contienen datos aleatorios y pueden contener datos personales. Los archivos se almacenan sin cifrar en el dispositivo en el que está instalado el Agente de red. Los archivos no se transfieren a Kaspersky automáticamente. El usuario puede transferir estos datos a Kaspersky manualmente a pedido del Servicio de soporte técnico para resolver problemas en la operación de Kaspersky Security Center.

Acerca de los documentos legales de Kaspersky Security Center Cloud Console

Para usar Kaspersky Security Center Cloud Console, debe leer y expresar su acuerdo con los términos y condiciones de los documentos legales especificados en el Sitio web de Kaspersky Security Center Cloud Console. Puede ver los términos y condiciones de la Política de privacidad de AO Kaspersky Lab para sitios web al iniciar sesión en Kaspersky Security Center Cloud Console para administrar un espacio de trabajo. Puede leer el Acuerdo de Kaspersky Security Center Cloud Console y el Acuerdo de procesamiento de datos de Kaspersky Security Center Cloud Console cuando cree un espacio de trabajo para la empresa.

Lea atentamente los textos de todos los documentos legales antes de comenzar a usar Kaspersky Security Center Cloud Console.

Contrato de licencia de usuario final para las aplicaciones de Kaspersky

El Contrato de licencia de usuario final (en lo sucesivo también denominado Contrato de licencia o EULA) es un acuerdo obligatorio entre AO Kaspersky Lab y usted que estipula las condiciones según las cuales puede utilizar las aplicaciones de Kaspersky.

Puede ver los términos del Contrato de licencia de usuario final mediante los siguientes métodos:

- En la ventana, que se muestra durante la creación del paquete de instalación de la aplicación de Kaspersky.
- En el archivo license.txt, en la carpeta de instalación de la aplicación de Kaspersky, en el dispositivo administrado.

Puede revocar su aceptación del Contrato de licencia de usuario final en cualquier momento.

Si no acepta los términos del Contrato de licencia para una aplicación de Kaspersky, no puede usar esta aplicación.

Guía de protección

Kaspersky Security Center Cloud Console es una aplicación alojada y mantenida por Kaspersky. No es necesario instalar Kaspersky Security Center Cloud Console en su ordenador o servidor. Kaspersky Security Center Cloud Console permite al administrador instalar aplicaciones de seguridad de Kaspersky en dispositivos en una red corporativa, ejecutar tareas de análisis y actualización de forma remota y administrar las directivas de seguridad de las aplicaciones administradas.

Kaspersky Security Center Cloud Console 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 Cloud Console le permite configurar todos los componentes de protección creados con las aplicaciones de Kaspersky.

Kaspersky Security Center Cloud Console 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 protección mejorados para Kaspersky Security Center Cloud Console.

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

La Guía de protección contiene la siguiente información:

- Configurar cuentas para acceder a Kaspersky Security Center Cloud Console
- Gestión de la protección de dispositivos cliente
- Configuración de la protección para aplicaciones administradas
- Transferencia de información a aplicaciones de terceros

Antes de comenzar a trabajar con Kaspersky Security Center Cloud Console, se le solicitará que lea la versión breve de la Guía para reforzar la seguridad.

Tenga en cuenta que mientras que no confirme que ha leído la Guía para reforzar la seguridad, no podrá usar el Servidor de administración.

Para leer la Guía de protección:

1. Abra Kaspersky Security Center Cloud Console e inicie sesión en ella. Kaspersky Security Center Cloud Console comprueba si ha confirmado la lectura de la versión actual de la Guía para reforzar la seguridad.

   Si aún no ha leído la Guía de protección, se abre una ventana y aparece una versión breve de la misma.

2. Realice una de las siguientes acciones:

   - Si desea ver la versión breve de la Guía para reforzar la seguridad como documento de texto, haga clic en el enlace **Abrir en una ventana nueva**.
   - Si desea ver la versión completa de la Guía para reforzar la seguridad, haga clic en el enlace **Abrir la Guía para reforzar la seguridad en la Ayuda en línea**.

3. Tras leer la Guía para reforzar la seguridad, marque la casilla **Confirmo que he leído y entiendo en su totalidad la Guía para reforzar la seguridad** y, a continuación, haga clic en el botón **Aceptar**.

Ahora, puede trabajar con Kaspersky Security Center Cloud Console.

Cuando aparece una nueva versión de la Guía para reforzar la seguridad, Kaspersky Security Center le solicita que la lea.

Planificar la arquitectura de Kaspersky Security Center Cloud Console

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 Cloud Console y su interacción entre sí, así como con esquemas de tráfico de datos y uso de puertos.

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

- Organización de los espacios de trabajo del administrador y métodos para conectarse a Kaspersky Security Center Cloud Console
- Métodos de despliegue del Agente de red y el software de protección
- Mediante puntos de distribución
- Mediante Servidores de administración virtuales
- Mediante una jerarquía de Servidores de administración
- esquema de actualización de la base de datos antivirus
- Otros flujos de información

Cuentas y autenticación

Usar la verificación en dos pasos con Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console proporciona la verificación en dos pasos para los usuarios.

La verificación en dos pasos puede ayudarle a mejorar la seguridad de su cuenta en Kaspersky Security Center Cloud Console. Cuando esta función está activada, cada vez que inicie sesión en Kaspersky Security Center Cloud Console con su dirección de correo electrónico y contraseña, introducirá un código de seguridad adicional de uso único. Puede recibir un código de seguridad de un solo uso por SMS o generar este código en su app de autenticación (según el método de verificación en dos pasos que haya configurado).

Desaconsejamos instalar la app de autenticación en el mismo dispositivo desde el que se establece la conexión con el Servidor de administración. Puede instalar una app de autenticación en su dispositivo móvil.

Prohibición de guardar la contraseña de administrador

Si utiliza Kaspersky Security Center Cloud Console, **desaconsejamos** guardar la contraseña de administrador en el navegador instalado en el dispositivo del usuario.

Si el navegador se ve afectado, un intruso puede obtener acceso a las contraseñas guardadas. Además, si un dispositivo de usuario con contraseñas guardadas resulta robado o perdido, un intruso puede obtener acceso a datos protegidos.

Restricción de la pertenencia a la función de Administrador principal

Recomendamos restringir la pertenencia a la función de Administrador principal.

De forma predeterminada, después de que un usuario crea un espacio de trabajo, se le asigna la función de Administrador principal. Es útil para la administración, pero su uso puede representar peligro desde el punto de vista de la seguridad, ya que la función de administrador principal tiene una amplia gama de privilegios. La asignación de esta función a los usuarios debe estar bajo estricta regulación.

Puede usar las funciones de usuario predefinidas con un conjunto de derechos preconfigurados para administrar Kaspersky Security Center Cloud Console.

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 Cloud Console para cada usuario o grupo de usuarios.

El control de acceso basado en funciones permite crear funciones de usuario estándar con un conjunto predefinido de derechos y asignar esos roles a los usuarios según el alcance de sus obligaciones.

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 determinados empleados según sus puestos o crear funciones completamente nuevas.

Al configurar las 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 una función o permisos a determinadas cuentas.

Gestión de la protección de dispositivos cliente

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 utiliza reglas automáticas para mover dispositivos, esto puede llevar a la propagación de directivas que proporcionen más privilegios al dispositivo movido de los que tenía el dispositivo 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 con el Agente de red instalado pueden actuar como un 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.
- Actuar como servidor proxy de KSN para dispositivos cliente.

Teniendo en cuenta las capacidades disponibles, recomendamos proteger los dispositivos que actúan como puntos de distribución frente a cualquier tipo de acceso no autorizado (incluido el físico).

Configuración de la protección para aplicaciones administradas

Configurar la protección de la red

Asegúrese de haber completado el escenario de configuración inicial de Kaspersky Security Center Cloud Console. Este escenario también incluye realizar los pasos del asistente de inicio rápido.

Cuando se ejecuta el asistente de inicio rápido, se crean directivas y tareas con parámetros predeterminados. Estos parámetros pueden no ser los mejores, o incluso estar prohibidos en su organización. Por lo tanto, recomendamos configurar las directivas y tareas creadas, y, de ser necesario, crear directivas y tareas adicionales para la red de su organización.

Especificación de la contraseña para desactivar la protección y desinstalar la aplicación

Para evitar que los intrusos desactiven las aplicaciones de protección de Kaspersky, recomendamos encarecidamente activar la protección con contraseña para desactivar la protección y la desinstalación de las aplicaciones de protección de Kaspersky. Puede configurar la contraseña, por ejemplo, para Kaspersky Endpoint Security for Windows, Kaspersky Security for Windows Server, Agente de red y otras aplicaciones de Kaspersky. Después de activar la protección con contraseña, recomendamos bloquear esta configuración cerrando el "candado".

Especificar la contraseña para la utilidad klmover y eliminar el Agente de red

Recomendamos encarecidamente activar la protección con contraseña para ejecutar la utilidad klmover y eliminar el Agente de red. Para activar la protección con contraseña, seleccione la opción **Utilizar contraseña de desinstalación** en la configuración de la directiva del Agente de red.

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

> La utilidad klmover se usa solo para mover dispositivos administrados bajo la administración de un Servidor de administración virtual. Al instalar el Agente de red en el dispositivo administrado, la utilidad klmover se copia automáticamente a la carpeta de instalación del Agente de red.

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 actualice Kaspersky Security Center Cloud Console, puede aceptar la Declaración de KSN actualizada.

Detección de nuevos dispositivos

Recomendamos establecer correctamente la configuración de detección de dispositivos: configure la integración con Active Directory y especifique intervalos de direcciones IP para detectar nuevos dispositivos.

Por motivos de seguridad, puede utilizar el grupo de administración predeterminado que incluye todos los dispositivos nuevos y las directivas predeterminadas que afectan a este grupo.

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

Para poder dar una respuesta oportuna ante emergencias, recomendamos configurar Kaspersky Security Center Cloud Console para enviar notificaciones sobre los eventos de auditoría, eventos críticos, eventos de fallos y advertencias que publique.

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.

Recomendaciones de seguridad para sistemas de información de terceros

Recomendaciones de seguridad de CIS Benchmarks

Al usar versiones de sistemas operativos o plataformas de virtualización compatibles con Agente de red, recomendamos aplicar las mejores prácticas de seguridad de la información del Center for Internet Security (CIS), si corresponde, para ajustar estos sistemas de información.

El Center for Internet Security (CIS) es una organización sin fines de lucro dedicada a mejorar la seguridad en el campo de la tecnología de la información. En particular, el CIS desarrolla y distribuye estándares de seguridad como CIS Controls y CIS Benchmarks. Estos estándares son un conjunto de recomendaciones y prácticas para garantizar la seguridad de los sistemas de información.

El portal del CIS contiene recomendaciones para las versiones de los siguientes sistemas de información compatibles con Agente de red:

- Sistemas operativos de las siguientes familias:
  - Windows para ordenadores de escritorio
  - Windows para servidores
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- Plataformas de virtualización VMware

Recomendaciones de seguridad para el sistema operativo Astra Linux

Al utilizar el sistema operativo Astra Linux, debe seguir las recomendaciones de seguridad descritas en el Libro rojo para la versión correspondiente de Astra Linux.

Recomendaciones para usar las aplicaciones de seguridad de Kaspersky

Uso de la contraseña de KLAdmin en Kaspersky Endpoint Security para Windows

Distintos usuarios con diferentes niveles de conocimientos informáticos pueden compartir un dispositivo con Kaspersky Endpoint Security para Windows instalado. Si los usuarios tienen acceso sin restricciones a Kaspersky Endpoint Security para Windows y sus configuraciones, el nivel general de protección del dispositivo puede verse reducido. La protección con contraseña le permite restringir el acceso de los usuarios a Kaspersky Endpoint Security para Windows en función de los permisos otorgados a ellos (por ejemplo, permiso para salir de la aplicación).

Una de las formas de restringir el acceso a Kaspersky Endpoint Security para Windows y sus parámetros es usar una cuenta KLAdmin. La cuenta KLAdmin es una cuenta de administrador con acceso irrestricto a Kaspersky Endpoint Security para Windows. La cuenta KLAdmin tiene derecho a realizar cualquier acción protegida con contraseña en Kaspersky Endpoint Security para Windows. Los permisos para la cuenta KLAdmin no pueden revocarse. Puede configurar la contraseña para la cuenta KLAdmin en las propiedades de la directiva de Kaspersky Endpoint Security para Windows. El administrador de Kaspersky Endpoint Security para Windows es plenamente responsable del uso seguro de la contraseña de la cuenta KLAdmin. Si su organización tiene su propia directiva de contraseñas, siga las instrucciones de esa directiva.

Nuestras recomendaciones para proteger a la organización contra el robo de la contraseña de KLAdmin son las siguientes:

- **Requisitos generales**

  No utilice el nombre de la cuenta ni parte del nombre de la cuenta como contraseña

- **Requisitos de longitud mínimos de la contraseña**

  Cree una contraseña de al menos 10 caracteres.

- **Requisitos para utilizar varios tipos de caracteres**

  Configure una contraseña compleja que incluya caracteres de diferentes categorías: letras en mayúscula y minúscula, números y caracteres especiales.

- **Requisitos de caducidad de la contraseña**

  Configure una fecha de caducidad mínima de la contraseña de 90 días La nueva contraseña no debe ser igual a ninguna de las 24 contraseñas anteriores.

Interfaz de Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console se administra a través de una interfaz web.

La ventana de la aplicación contiene los siguientes elementos:

- Menú principal en la parte izquierda de la ventana
- Área de trabajo en la parte derecha de la ventana

Menú principal

El menú principal contiene las siguientes secciones:

- **Enlaces rápidos**. Contiene las siguientes pestañas:
  - **Ajustes de la página de inicio**. Muestra el mapa del menú principal. De forma predeterminada, la pestaña **Ajustes de la página de inicio** de la sección **Enlaces rápidos** está configurada como página de inicio. Puede cambiar esta configuración.
  - **Introducción y tutoriales**. Vídeos sobre cómo configurar y usar Kaspersky Security Center Cloud Console y las aplicaciones de seguridad.

    En el navegador Mozilla Firefox, si reproduce un video en la sección **Introducción y tutoriales** en la ventana emergente, y después abre el vídeo en el modo de imagen en imagen, y luego lo cierra en la ventana emergente, el video en el modo imagen en imagen también se cerrará.
- **Servidor de administración**. Muestra el nombre del Servidor de administración al que está conectado actualmente. Haga clic en el icono de configuración ( ) para abrir las propiedades del Servidor de administración.
- **Control e informes**. Estas capacidades le brindan una visión general de su infraestructura, estados de protección y estadísticas.
- **Activos (dispositivos)**. Contiene herramientas para administrar dispositivos cliente, así como tareas y directivas de la aplicación de Kaspersky.
- **Usuarios y funciones**. Le permite administrar usuarios y roles, configurar derechos de usuario asignando roles a los usuarios y asociar perfiles de directivas con roles.
- **Operaciones**. Contiene una variedad de operaciones, entre ellas las licencias de aplicaciones, la administración de parches y la administración de aplicaciones de terceros. Esto también le proporciona acceso a los repositorios de aplicaciones.
- **Detección y despliegue**. Le permite sondear la red para descubrir dispositivos cliente y distribuir los dispositivos a grupos de administración de forma manual o automática. También contiene el asistente de inicio rápido y el asistente de despliegue de la protección.
- **Marketplace**. Contiene información sobre la gama completa de soluciones comerciales de Kaspersky y le permite seleccionar las que necesita y luego comprar esas soluciones en el sitio web de Kaspersky.
- **Configuración**. Contiene ajustes para integrar Kaspersky Security Center Cloud Console con otras aplicaciones de Kaspersky. También contiene su configuración personal relacionada con la apariencia de la

interfaz, como el tema o el idioma de la interfaz.

- **El menú de su cuenta**. Contiene un enlace a la Ayuda en línea e información sobre el Soporte técnico de Kaspersky. También le permite cerrar sesión en Kaspersky Security Center Cloud Console.

Área de trabajo

El área de trabajo muestra la información que elige ver en las secciones de la ventana de la interfaz web de la aplicación. También contiene elementos de control que puede utilizar para configurar cómo se muestra la información.

Cambiar el idioma de la interfaz de Kaspersky Security Center Cloud Console

Puede seleccionar el idioma de la interfaz de Kaspersky Security Center Cloud Console.

Para cambiar el idioma de la interfaz:

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

Cambiar la página de inicio de Kaspersky Security Center Cloud Console

La página de inicio se muestra después de iniciar sesión en Kaspersky Security Center Cloud Console.

De forma predeterminada, la pestaña **Ajustes de la página de inicio** de la sección **Enlaces rápidos** se establece como página de inicio. Si es necesario, puede cambiar la página de inicio.

Para cambiar la página de inicio:

1. En la sección **Enlaces rápidos**, pase el cursor del mouse sobre el elemento que desea establecer como página de inicio.
2. Cuando aparezca el icono de inicio (), haga clic en él.

Se cambia la página de inicio, se muestra un mensaje apropiado en la pantalla y el elemento seleccionado como página de inicio se marca con el icono inicio ().

Las secciones **Marketplace** y **Configuración** no se pueden establecer como página de inicio.

Añadir y eliminar marcadores

Puede añadir secciones de uso frecuente de Kaspersky Security Center Cloud Console a marcadores para acceder a ellas rápidamente desde la sección **Marcadores** del menú principal.

Si no ha añadido ninguna sección a los marcadores, la sección **Marcadores** no aparece en el menú principal.

Puede añadir a marcadores sólo las secciones que muestran páginas. Por ejemplo, si va a **Activos (dispositivos)** → **Dispositivos administrados**, se abre una página con la tabla de dispositivos, lo que significa que puede añadir la sección **Dispositivos administrados** a los marcadores. Si se muestra una ventana o no se muestra ningún elemento después de seleccionar la sección en el menú principal, no puede añadir dicha sección a los marcadores.

Para añadir una sección a los marcadores:

1. En el menú principal, pase el cursor del ratón sobre la sección que desea añadir a los marcadores.
2. Después del marcador (🔖) se muestra el ícono, haga clic en el ícono.

   Esta sección aparece en la sección **Marcadores**.

Para eliminar una sección de los marcadores:

1. En el menú principal, vaya a la sección **Marcadores**.
2. Pase el cursor del ratón sobre la sección que desea desanclar y haga clic en el ícono de desanclar (🔖).

   La sección se elimina de los marcadores.

También puede añadir y eliminar elementos de los marcadores de la sección **Enlaces rápidos** situando el cursor del ratón sobre ellas y haciendo clic en el icono del marcador (🔖). El elemento seleccionado se marcará con el icono de marcador (🔖) y aparecerá en la sección **Marcadores** del menú principal. Si desea eliminar el elemento de los marcadores, haga clic en el ícono (🔖).

La sección **Marcadores** se muestra solo en el menú principal. Nunca aparece en la página de **Enlaces rápidos**.

Configuración inicial de Kaspersky Security Center Cloud Console

Esta sección describe el escenario principal para el despliegue de Kaspersky Security Center Cloud Console, que comienza con la creación de un espacio de trabajo y termina con la supervisión del estado de la protección de la red.

Para obtener información sobre el despliegue de Kaspersky Security Center en las instalaciones, consulte la Ayuda en línea de Kaspersky Security Center.

Le recomendamos que asigne un mínimo de un día hábil para completar este escenario.

El escenario lo guía a través de lo siguiente:

- Comenzar a trabajar con un espacio de trabajo de su empresa como administrador.
- Descubrir dispositivos en su red; si es necesario, asignará puntos de distribución e instalará de forma manual paquetes de distribución en ellos.
- Instalar aplicaciones de Kaspersky administradas en los dispositivos cliente y configurar herramientas para la protección y la supervisión de la red y las actualizaciones periódicas de las bases de datos, módulos de software y aplicaciones de Kaspersky.

Cuando complete este escenario, se configurará la protección de red basada en las aplicaciones de Kaspersky. Podrá continuar con la supervisión del estado de la protección de la red.

Requisitos previos

Antes de comenzar:

- Vea la arquitectura de Kaspersky Security Center Cloud Console para comprender la interacción entre los componentes principales de aplicación.
- Lea la información sobre las licencias de Kaspersky Security Center Cloud Console y las aplicaciones administradas.
- Asegúrese de tener un código de activación válido para Kaspersky Security Center Cloud Console (si creará un espacio de trabajo comercial).

Etapas

La configuración de Kaspersky Security Center Cloud Console se realiza en etapas:

1. **Configure los puertos**

   Asegúrese de que todos los puertos necesarios estén abiertos para la interacción entre la red y la infraestructura de Kaspersky. Además, si planea utilizar la jerarquía de Servidores de administración, asegúrese de que todos los puertos necesarios estén abiertos para la interacción entre el Servidor de administración secundario (o Servidores de administración secundarios) y los dispositivos cliente.

2. **Creación del espacio de trabajo para su empresa**

   Cree una cuenta y, luego, cree un espacio de trabajo para su empresa.

3. **Ejecución del asistente de inicio rápido**

Abra e inicie sesión en Kaspersky Security Center Cloud Console. Cuando inicie sesión por primera vez, se le solicitará automáticamente que ejecute el asistente de inicio rápido. También puede iniciar el asistente de inicio rápido manualmente en cualquier momento.

Cuando se complete el asistente de inicio rápido, tendrá paquetes de instalación del Agente de red y las aplicaciones de seguridad. Estos paquetes de instalación son necesarios para avanzar con el despliegue de Kaspersky Security Center Cloud Console.

4. **Despliegue de las aplicaciones de Kaspersky**

   Realice el escenario de despliegue inicial de las aplicaciones de Kaspersky. Uno de los pasos del escenario se refiere a la operación de sondeo de red. Esta operación es necesaria para descubrir los dispositivos cliente de la red. El sondeo de red y su configuración se describen en el escenario de descubrimiento de dispositivos en red.

   Si está desplegando Kaspersky Security for Windows Server, asegúrese de que las bases de datos de esta aplicación estén actualizadas.

5. **Licencias de las aplicaciones de seguridad de Kaspersky**

   Cuando las aplicaciones de seguridad de Kaspersky se despliegan en los dispositivos administrados, se deben licenciar aplicando un código de activación a cada una de las aplicaciones. Despliegue los códigos de activación en las aplicaciones de Kaspersky instaladas en los dispositivos administrados. Tiene varias opciones para licenciar las aplicaciones de seguridad de Kaspersky.

6. **Configurar la protección de la red**

   Realice la configuración de protección de red para configurar con más precisión las directivas y tareas creadas por medio del asistente de inicio rápido.

7. **Actualizar periódicamente las bases de datos, los módulos de software y las aplicaciones de Kaspersky**

   Para mantener su red protegida contra virus y otras amenazas, tiene que configurar actualizaciones periódicas de las bases de datos, los módulos de software y las aplicaciones de Kaspersky.

8. **Actualización de software de terceros y corrección de vulnerabilidades de software de terceros (opcional)**

   Kaspersky Security Center Cloud Console le permite administrar las actualizaciones de las aplicaciones de Microsoft instaladas en los dispositivos cliente. También puede usarse para reparar las vulnerabilidades presentes en las aplicaciones de Microsoft a través de la instalación de las actualizaciones requeridas.

9. **Configuración de herramientas para supervisar el estado de la protección de la red**

   Seleccione y configure widgets, informes y otras herramientas que le permitan supervisar el estado de la protección de la red.

Una vez que se despliega y configura Kaspersky Security Center Cloud Console, puede proceder a supervisar el estado de la protección de la red.

Administración de los espacios de trabajo

Esta sección describe cómo puede usar cuentas y espacios de trabajo en Kaspersky Security Center Cloud Console.

Acerca de la administración de los espacios de trabajo en Kaspersky Security Center Cloud Console

Con Kaspersky Security Center Cloud Console, puede hacer lo siguiente:

- Crear una cuenta.
- Editar una cuenta.
- Registrar una empresa y crear un espacio de trabajo.
- Editar información sobre la empresa y los espacios de trabajo.
- Eliminar un espacio de trabajo y una empresa.
- Eliminar una cuenta.

Guía de inicio rápido de Kaspersky Security Center Cloud Console

En esta sección se describe cómo registrarse y comenzar a usar Kaspersky Security Center Cloud Console.

Registrarse en Kaspersky Security Center Cloud Console consta de los siguientes pasos:

1. Crear y confirmar una cuenta.
2. Registrar una empresa y crear un espacio de trabajo.

Crear una cuenta

En este artículo, se describe cómo crear una cuenta en Kaspersky Security Center Cloud Console.

También puede crear una cuenta en My Kaspersky y, luego, usarla para iniciar sesión en Kaspersky Security Center Cloud Console y crear su espacio de trabajo.

> Su cuenta de My Kaspersky debe crearse directamente en el sitio web y no a través de un proveedor de autenticación externo (como Google). De lo contrario, no podrá utilizar Kaspersky Security Center Cloud Console.

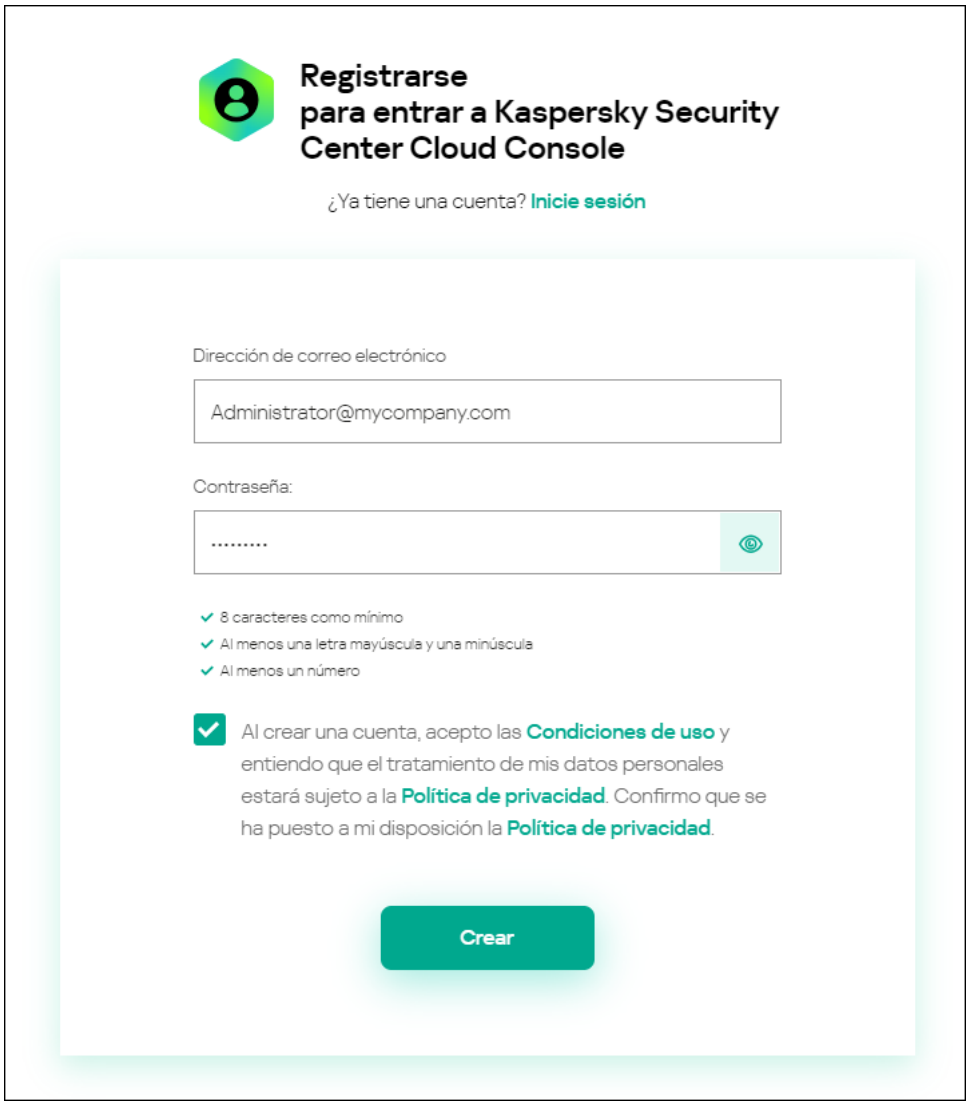
Para crear una cuenta en Kaspersky Security Center Cloud Console:

1. En el navegador, vaya a Kaspersky Security Center Cloud Console.

2. Haga clic en el botón **Cree una cuenta**, en la página de inicio de Kaspersky Security Center Cloud Console.

   Se abre el portal de Kaspersky Account.

3. En la página **Regístrese para ingresar a Kaspersky Security Center Cloud Console**, ingrese la dirección de correo electrónico y la contraseña de su cuenta (consulte la figura a continuación).



Crear una cuenta en Kaspersky Security Center Cloud Console

4. Haga clic en el vínculo **Política de privacidad** y lea atentamente el texto de la Directiva de privacidad.

5. Si entiende y acepta que sus datos serán tratados y transmitidos (incluso a terceros países) como se describe en la Política de privacidad y confirma que ha leído y entendido la Política de privacidad en su totalidad, marque la casilla junto al texto de consentimiento al procesamiento de datos de acuerdo con la Política de privacidad, y luego haga clic en el botón **Crear**.

   Si no acepta la Política de privacidad, no use Kaspersky Security Center Cloud Console.

6. Un mensaje de Kaspersky se envía a la dirección de correo electrónico que especificó. El mensaje contiene un código de seguridad de un solo uso.

   Abra el mensaje de correo electrónico y copie el código de seguridad de un solo uso que contiene.

7. Vuelva a Kaspersky Account y pegue el código en el campo de entrada.

La creación de la cuenta en Kaspersky Security Center Cloud Console queda completa.

Registro de una empresa y creación de un espacio de trabajo

Inmediatamente después de crear la cuenta, puede registrar una empresa y crear un espacio de trabajo para ella.

Si necesita proteger más de 10000 dispositivos, no tiene que seguir las instrucciones que se detallan a continuación para registrar una empresa y crear un espacio de trabajo en Kaspersky Security Center Cloud Console. En su lugar, envíe una solicitud al Servicio de soporte técnico de Kaspersky. En la solicitud, especifique la información de su empresa y el espacio de trabajo que desea crear.

Antes de iniciar, asegúrese de saber lo siguiente:

- El nombre de la empresa en la que va a usar la solución de software.
- El país donde se encuentra la empresa. Si la empresa está ubicada en Canadá, también debe conocer la provincia.
- La cantidad total de equipos y dispositivos móviles de la empresa que desea proteger.

Para registrar una empresa y crear un espacio de trabajo en Kaspersky Security Center Cloud Console, haga lo siguiente:

1. En el navegador, vaya a Kaspersky Security Center Cloud Console.
2. Haga clic en el botón **Iniciar sesión** de la página de inicio de Kaspersky Security Center Cloud Console.
3. Escriba la dirección de correo electrónico y la contraseña que especificó cuando creó la cuenta y haga clic en el botón **Iniciar sesión**.

   Se inicia el Asistente para crear un espacio de trabajo. Avance por el asistente utilizando el botón **Next**.
4. En la página del asistente **Paso 01: Condiciones de uso de Kaspersky Security Center Cloud Console**, haga lo siguiente:

   a. Lea con atención el Contrato, la Política de privacidad y el Contrato de procesamiento de datos de la solución de software.

   b. Si acepta los términos y las condiciones del Contrato y del Contrato de procesamiento de datos, entiende y acepta que sus datos se administrarán y se transmitirán (incluso a otros países) como se describe en la Política de privacidad y confirma que ha leído y entiende la Política de privacidad en su totalidad, seleccione las casillas que están junto a los tres documentos enumerados y haga clic en el botón **Aceptar**.

   Si no acepta los términos y las condiciones, no use Kaspersky Security Center Cloud Console.

   Si hace clic en el botón **Rechazar**, el proceso de creación del espacio de trabajo finalizará.
5. En la página del asistente **Paso 02: Información sobre la empresa**, especifique la información principal de su empresa.

   Rellene los siguientes campos:

   - **Nombre de su empresa** (obligatorio).

Especifique el nombre de la empresa en la cual tiene la intención de usar la solución de software. Puede introducir una cadena de 255 caracteres máximo. La cadena puede contener caracteres en mayúsculas y minúsculas, números, espacios en blanco, puntos, comas, signos menos, guiones y guiones bajos. El nombre de la empresa especificado se mostrará en Kaspersky Security Center Cloud Console.

- Campo **Descripción adicional de la empresa** (opcional).

  Puede especificar información adicional sobre la empresa que registre. Puede escribir una cadena de hasta 255 caracteres. La cadena puede contener caracteres en mayúsculas y minúsculas, números, espacios en blanco, puntos, comas, signos menos, guiones y guiones bajos.

6. En la página del asistente **Paso 03: Información sobre el espacio de trabajo**, especifique la información sobre el espacio de trabajo que desea crear para la empresa.

   Complete los siguientes campos obligatorios:

   - **Nombre del espacio de trabajo**. Especifique el nombre del espacio de trabajo en el que va a usar la solución de software. Puede escribir una cadena de hasta 255 caracteres. La cadena puede contener caracteres en mayúsculas y minúsculas, números, espacios en blanco, puntos, comas, signos menos, guiones y guiones bajos. El nombre del espacio de trabajo especificado se mostrará en Kaspersky Security Center Cloud Console.

   - **País**. En la lista desplegable, seleccione el país en el que está ubicado el espacio de trabajo. Si selecciona Canadá, también especifique la provincia en la lista desplegable **Estado** que aparece a continuación de este campo.

   - **Número de dispositivos**. Escriba la cantidad total de equipos y dispositivos móviles que desea proteger en este espacio de trabajo.

     En el campo de entrada, se puede introducir un número entre 20 y 10 000. La cantidad mínima exacta de dispositivos que puede proteger depende de la licencia que haya adquirido.

7. En la página del asistente **Paso 04: Licencia para un nuevo espacio de trabajo**, realice una de las siguientes acciones:

   - Si desea probar Kaspersky Security Center Cloud Console, haga clic en el enlace **Quiero solicitar un espacio de trabajo de prueba**.

     Recomendamos que conecte sus propios dispositivos al espacio de trabajo de prueba y pruebe cualquier modificación en la configuración, anotando los resultados.

     No podrá cambiar un espacio de trabajo de prueba al modo comercial mediante el ingreso de un código de activación. Para cambiar al modo comercial, debe eliminar el espacio de trabajo y volver a crearlo.

   - Si desea utilizar Kaspersky Security Center Cloud Console en el modo comercial, introduzca el código de activación y haga clic en el botón **Verificar**.

El registro de la empresa y la creación de un espacio de trabajo en Kaspersky Security Center Cloud Console está completo.

Después de la preparación del espacio de trabajo, recibirá un mensaje de correo electrónico con el enlace para acceder al espacio de trabajo.

Proteger más de 10 000 dispositivos

Si desea proteger más de 10 000 dispositivos, no es necesario registrar una empresa y crear un espacio de trabajo. En su lugar, envíe una solicitud al Servicio de soporte técnico de Kaspersky. El número máximo de dispositivos por espacio de trabajo es de 25 000.

La solicitud debe contener la siguiente información:

- **Correo electrónico del usuario**: la dirección de correo electrónico del usuario que se registró en Kaspersky Security Center Cloud Console. Este usuario recibe derechos de administrador en el espacio de trabajo creado.

  Puede crear una cuenta en Kaspersky Security Center Cloud Console y no registrar una empresa ni crear un espacio de trabajo para ella. Especifique información sobre la empresa y el espacio de trabajo en la solicitud.

- **Nombre de empresa**: el nombre de la empresa en la que desea utilizar Kaspersky Security Center Cloud Console.

- **País de la empresa**: el país en el que se encuentra la empresa.

- **Nombre del espacio de trabajo**: el nombre del espacio de trabajo que se creará para la empresa.

- **Número estimado de endpoints**: el número total de dispositivos cliente (incluidos los dispositivos móviles) que desea proteger en el nuevo espacio de trabajo.

- **País del espacio de trabajo**: el país en el que desea ubicar su nuevo espacio de trabajo. Este parámetro afecta la selección del centro de datos donde se almacena el espacio de trabajo.

  Los parámetros **País de la empresa** y **País del espacio de trabajo** pueden ser los mismos.

- **Código de activación**: el código de activación que recibe después de comprar Kaspersky Security Center Cloud Console. Cerciórese de que la licencia que desea comprar cubra todos los dispositivos cliente que deben protegerse.

Después de enviar la solicitud, los especialistas de Kaspersky registran la empresa especificada y crean un espacio de trabajo para ella. Cuando se complete la creación del espacio de trabajo, recibirá una notificación por correo electrónico. Para ver el resultado de su solicitud, inicie sesión con su cuenta en Kaspersky Security Center Cloud Console.

Apertura del espacio de trabajo en Kaspersky Security Center Cloud Console

Inmediatamente después de crear un espacio de trabajo para Kaspersky Security Center Cloud Console, el espacio de trabajo se abre de forma automática. Más adelante, puede abrir el espacio de trabajo, como se indica en esta sección.

Si es un administrador de un Servidor de Administración virtual, solo tiene acceso al Servidor de administración virtual. Después de iniciar sesión y abrir el espacio de trabajo, Kaspersky Security Center Cloud Console le proporciona la interfaz del Servidor de administración virtual. No puede cambiar al Servidor de administración principal ni a otros Servidores de administración secundarios.

> Un administrador de un Servidor de administración virtual debe tener acceso a un solo Servidor de administración virtual. Si no tiene derechos de acceso en el servidor principal y tiene derechos de acceso en varios servidores virtuales, no puede iniciar sesión en Kaspersky Security Center Cloud Console.

Para abrir el espacio de trabajo de Kaspersky Security Center Cloud Console:

1. En su navegador, vaya a Kaspersky Security Center Cloud Console.
2. Para iniciar sesión con su cuenta en Kaspersky Security Center Cloud Console, especifique el nombre de usuario y la contraseña.
3. Si configura la verificación en dos pasos, introduzca el código de seguridad de uso único que ha recibido por SMS o que generó en la app de autenticación (según el método de verificación en dos pasos que haya configurado).

   La página del portal muestra la empresa de la que usted es administrador y la lista de sus espacios de trabajo.
4. Haga clic en el nombre del espacio de trabajo requerido o el enlace **Ir al espacio de trabajo** para acceder al espacio de trabajo.

   En algunas ocasiones, un espacio de trabajo puede no estar disponible por estar en mantenimiento. Si es así, no podrá acceder al espacio de trabajo de Kaspersky Security Center Cloud Console.

   > No puede abrir un espacio de trabajo que esté marcado para su eliminación.
5. Si cualquiera de los documentos legales de Kaspersky Security Center Cloud Console se han modificado desde que aceptó sus términos y condiciones, la página del portal mostrará los documentos modificados.

   Haga lo siguiente:

   a. Lea con atención los documentos en pantalla.

   b. Si acepta los términos y las condiciones de los documentos que se muestran, seleccione las casillas de verificación que están junto a los documentos y, luego, haga clic en el botón **Acepto las condiciones**.

   > Si no acepta los términos y condiciones, deje de usar la solución de software de Kaspersky seleccionada.

   > Si hace clic en el botón **No acepto**, finalizará la operación.

Se abre el espacio de trabajo de Kaspersky Security Center Cloud Console.

Regreso a la lista de espacios de trabajo

Después de abrir su espacio de trabajo, puede volver a la página del portal que tiene la lista de espacios de trabajo registrados en su cuenta en Kaspersky Security Center Cloud Console.

Para volver a la lista de espacios de trabajo, haga lo siguiente:

En el menú principal, vaya a la configuración de la cuenta y, a continuación, elija **Administrar espacios de trabajo**.

La página del portal muestra la empresa de la que usted es administrador y la lista de sus espacios de trabajo. Si abrió Kaspersky Security Center Cloud Console en varias pestañas, se cerrará la sesión en todas ellas.

Cerrar sesión en Kaspersky Security Center Cloud Console

Cuando haya terminado su trabajo, debe cerrar de forma segura su sesión. Para ello, cierre la sesión en Kaspersky Security Center Cloud Console.

Para cerrar sesión en Kaspersky Security Center Cloud Console:

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

Kaspersky Security Center Cloud Console se cierra y se muestra la página de inicio de sesión. De ser necesario, puede cerrar esta página del navegador. Se guardarán todos los datos de su espacio de trabajo.

Administración de la empresa y la lista de espacios de trabajo

Esta sección describe cómo ver la información de la compañía y la lista de espacios de trabajo registrados bajo su cuenta en Kaspersky Security Center Cloud Console, cambiar la información sobre la compañía y los espacios de trabajo, y eliminar un espacio de trabajo y una compañía.

Actualmente, solo puede registrar una empresa y crear un espacio de trabajo. En futuras versiones de Kaspersky Security Center Cloud Console, podrá crear espacios de trabajo adicionales para su empresa. Esto le ayudará a trazar la estructura de la empresa en los espacios de trabajo, al crear un espacio de trabajo separado para cada sucursal de la empresa.

Modificar información sobre una empresa y un espacio de trabajo.

Puede modificar la información sobre una empresa y un espacio de trabajo que especificó al añadir la empresa a Kaspersky Security Center Cloud Console.

Para modificar información sobre una empresa y / o un espacio de trabajo:

1. En el navegador, vaya a Kaspersky Security Center Cloud Console.
2. Para iniciar sesión con su cuenta en Kaspersky Security Center Cloud Console, especifique el nombre de usuario y la contraseña.
3. Si configuró la verificación en dos pasos, introduzca el código de seguridad único que se le envió mediante SMS o que generó la aplicación de autenticación (según el método de verificación en dos pasos que haya configurado).

   La página del portal muestra la empresa de la que es administrador y una lista de sus espacios de trabajo.
4. Si desea editar el nombre y la descripción de la empresa, haga lo siguiente:
   a. Haga clic en el ícono **Editar** (✎) en el área con la información de la empresa.
   b. Modifique el nombre o la descripción de la empresa como desee.
   c. Haga clic en el botón **Guardar**.

      Para cancelar los cambios, haga clic en el botón **Cancelar**.
5. Si desea editar el nombre del espacio de trabajo, haga lo siguiente:
   a. Haga clic en el ícono **Editar** (✎) en el área con la información del espacio de trabajo.

b. Modifique el nombre del espacio de trabajo como desee.

c. Haga clic en el botón **Guardar**.

Para cancelar los cambios, haga clic en el botón **Cancelar**.

La información modificada se muestra en Kaspersky Security Center Cloud Console.

Eliminar un espacio de trabajo y una empresa

El espacio de trabajo de una empresa se puede eliminar de forma manual o automática. Después de eliminar el último espacio de trabajo, la información de la empresa también se elimina automáticamente.

Detección manual

Puede eliminar un espacio de trabajo de una empresa si esta ha decidido dejar de usar el espacio de trabajo.

Después de eliminar el espacio de trabajo, todas las aplicaciones de seguridad permanecerán en los dispositivos administrados. Por lo tanto, recomendamos que antes de eliminar el espacio de trabajo desactive la protección con contraseña de todas las aplicaciones de seguridad o desinstale las aplicaciones de seguridad de los dispositivos administrados.

Para eliminar un espacio de trabajo y una empresa:

1. En el navegador, vaya a Kaspersky Security Center Cloud Console.
2. Para iniciar sesión con su cuenta en Kaspersky Security Center Cloud Console, especifique el nombre de usuario y la contraseña.
3. Si configuró la verificación en dos pasos, introduzca el código de seguridad único que se le envió mediante SMS o que generó la aplicación de autenticación (según el método de verificación en dos pasos que haya configurado).

   La página del portal muestra la empresa de la que es administrador y una lista de sus espacios de trabajo.
4. Seleccione el espacio de trabajo que desea eliminar.
5. A la derecha, en la sección que contiene el espacio de trabajo seleccionado, haga clic en el icono **Eliminar** (🗑).

   Se abrirá la ventana **Eliminar espacio de trabajo**.
6. En la ventana **Eliminar espacio de trabajo**, confirme que desea eliminar el espacio de trabajo.

   El espacio de trabajo se marca para su eliminación. El bloque de información del espacio de trabajo se resalta con un borde rojo.

   El bloque de información del espacio de trabajo se duplica al pie de la página, en la sección **Marcado para su eliminación**.

No puede ir a un espacio de trabajo marcado para su eliminación y administrarlo.

Si no ha podido marcar un espacio de trabajo para eliminarlo, póngase en contacto con el Servicio de soporte técnico de Kaspersky. Cuando un ingeniero del Servicio de soporte técnico de Kaspersky reciba su solicitud, se eliminarán el espacio de trabajo y la empresa.

Los espacios de trabajo marcados para su eliminación pueden permanecer en ese estado durante un período de siete días después de marcarlos. Después de siete días, se eliminan automáticamente.

Durante ese período, puede eliminar a la fuerza un espacio de trabajo que está marcado para eliminarlo o cancelar la eliminación de un espacio de trabajo.

Para eliminar por la fuerza un espacio de trabajo:

1. En el navegador, vaya a Kaspersky Security Center Cloud Console.
2. Para iniciar sesión con su cuenta en Kaspersky Security Center Cloud Console, especifique el nombre de usuario y la contraseña.
3. Si configuró la verificación en dos pasos, introduzca el código de seguridad único que se le envió mediante SMS o que generó la aplicación de autenticación (según el método de verificación en dos pasos que haya configurado).

   La página del portal muestra la empresa de la que es administrador y una lista de sus espacios de trabajo.
4. En la sección **Marcado para su eliminación**, en el bloque de información del espacio de trabajo marcado para eliminar, haga clic en la opción **Forzar eliminación**.

   Se abrirá la ventana **Eliminar espacio de trabajo**.
5. En la ventana **Eliminar espacio de trabajo**, introduzca el Id. del espacio de trabajo que desea eliminar.

   Se le solicita que confirme el Id. del espacio de trabajo para asegurarse de que no elimine equivocadamente el espacio de trabajo. Una vez eliminado un espacio de trabajo, no se puede restaurar.

   El Id. de espacio de trabajo se muestra en la sección de información del espacio de trabajo debajo de su nombre.
6. En la ventana **Eliminar espacio de trabajo**, haga clic en **Aceptar**.

El espacio de trabajo se elimina. Todos los datos sobre los usuarios, dispositivos administrados y su configuración se eliminan.

Eliminación automática

Kaspersky Security Center Cloud Console elimina automáticamente un espacio de trabajo:

- 30 días después de caducar la licencia de prueba.
- 90 días después de caducar todas las licencias comerciales o de suscripción en el repositorio del Servidor de administración.
- 90 días después de eliminar la última clave de licencia (activa, de reserva o no en uso) añadida manualmente en el repositorio.

Kaspersky Security Center Cloud Console notifica a los administradores del espacio de trabajo 30 días, 7 días y 1 día antes de la eliminación.

Cancelar la eliminación de un espacio de trabajo

Puede cancelar la eliminación de un espacio de trabajo que se ha marcado para su eliminación.

No puede cancelar la eliminación de un espacio de trabajo que ya se ha eliminado.

Para cancelar la eliminación de un espacio de trabajo:

1. En el navegador, vaya a Kaspersky Security Center Cloud Console.
2. Para iniciar sesión con su cuenta en Kaspersky Security Center Cloud Console, especifique el nombre de usuario y la contraseña.
3. Si configuró la verificación en dos pasos, introduzca el código de seguridad único que se le envió mediante SMS o que generó la aplicación de autenticación (según el método de verificación en dos pasos que haya configurado).

   La página del portal muestra la empresa de la que es administrador y una lista de sus espacios de trabajo.
4. En la sección **Marcado para su eliminación**, en el bloque de información para el espacio de trabajo marcado para la eliminación, haga clic en el enlace **Cancelar eliminación**.

La eliminación del espacio de trabajo se cancela. Ahora puede ir al espacio de trabajo y continuar trabajando con él.

Administrar el acceso a la empresa y sus espacios de trabajo

Esta sección contiene información sobre cómo otorgar y revocar el acceso a su empresa y sus espacios de trabajo.

Kaspersky Security Center Cloud Console le proporciona dos niveles de acceso:

- **Administrador**

  Un usuario con este nivel de acceso puede administrar completamente la empresa y sus espacios de trabajo.
- **Usuario**

  Un usuario con este nivel de acceso puede ver la lista de espacios de trabajo disponibles y entrar a estos espacios de trabajo.

Conceder acceso a su empresa y sus espacios de trabajo

Puede otorgar acceso a su empresa y sus espacios de trabajo si desea que otro usuario pueda iniciar sesión en su empresa y administrarla según el nivel de acceso seleccionado.

Antes de poder otorgar acceso a un usuario, el usuario debe crear una cuenta en Kaspersky Security Center Cloud Console.

Para otorgar acceso a su empresa y sus espacios de trabajo:

1. En su navegador, vaya a Kaspersky Security Center Cloud Console.
2. Para iniciar sesión con su cuenta en Kaspersky Security Center Cloud Console, especifique el nombre de usuario y la contraseña.
3. Si configuró la verificación en dos pasos, introduzca el código de seguridad único que se le envió mediante SMS o que generó la aplicación de autenticación (según el método de verificación en dos pasos que haya configurado).

   La página del portal muestra la empresa de la que es administrador y una lista de sus espacios de trabajo.
4. Haga clic en el enlace **Mostrar control de acceso**.

   Se expande la lista de cuentas con acceso a la empresa.
5. Haga clic en el enlace **Otorgar acceso**.
6. En el campo **Dirección de correo electrónico**, especifique la dirección de correo electrónico de la cuenta a la que desea otorgar acceso.
7. En la lista **Nivel de acceso**, seleccione el nivel de acceso que desea asignar a la cuenta ingresada.

   - **Administrador**

     Un usuario con este nivel de acceso puede administrar completamente la empresa y sus espacios de trabajo.

   - **Usuario**

     Un usuario con este nivel de acceso puede ver la lista de espacios de trabajo disponibles y entrar a estos espacios de trabajo.

   No puede otorgar varios niveles de acceso a la misma cuenta dentro de la misma empresa.
8. Haga clic en el botón **Otorgar**.

La cuenta especificada recibe acceso a su empresa y sus espacios de trabajo. El usuario puede iniciar sesión en la empresa y administrarla según el nivel de acceso seleccionado.

Si otorgó el nivel de acceso de **Usuario** a la cuenta, debe asignar una función al usuario añadido. De lo contrario, el usuario no podrá ingresar al espacio de trabajo.

Revocar el acceso a su empresa y sus espacios de trabajo

Puede revocar el acceso a su empresa y sus espacios de trabajo si ya no desea que un usuario pueda iniciar sesión en su empresa y administrarla (por ejemplo, cuando el usuario abandona la empresa).

No puede revocar su propio acceso a la empresa.

Para revocar el acceso a su empresa y sus espacios de trabajo:

1. En su navegador, vaya a Kaspersky Security Center Cloud Console.
2. Para iniciar sesión con su cuenta en Kaspersky Security Center Cloud Console, especifique el nombre de usuario y la contraseña.
3. Si configuró la verificación en dos pasos, introduzca el código de seguridad único que se le envió mediante SMS o que generó la aplicación de autenticación (según el método de verificación en dos pasos que haya configurado).

   La página del portal muestra la empresa de la que es administrador y una lista de sus espacios de trabajo.
4. Haga clic en el enlace **Mostrar control de acceso**.

   Se expande la lista de cuentas con acceso a la empresa.
5. Haga clic en el icono **Revocar** (🗑) junto a la cuenta cuyo acceso desea revocar.
6. En la ventana **Revocar acceso a la empresa** que se abre, haga clic en **Aceptar** para confirmar la operación.

Se revoca el acceso a su empresa y sus espacios de trabajo de la cuenta seleccionada. El usuario ya no puede iniciar sesión en la empresa ni administrarla.

Restablecimiento de la contraseña

Si olvida la contraseña de su cuenta de Kaspersky Security Center Cloud Console, puede restaurar el acceso a la cuenta restableciendo la contraseña.

Para restablecer la contraseña de la cuenta:

1. En su navegador, vaya a Kaspersky Security Center Cloud Console.
2. Haga clic en el botón **Iniciar sesión**.
3. En la ventana **Iniciar sesión en Kaspersky Security Center Cloud Console** del portal Kaspersky Account que aparece, haga clic en el enlace **¿Ha olvidado su contraseña?**.
4. Introduzca la dirección de correo electrónico que especificó al crear la cuenta.
5. Haga clic en **Siguiente**.
6. Un mensaje de Kaspersky se envía a la dirección de correo electrónico que especificó. El mensaje contiene un código de seguridad de un solo uso.

   Abra el mensaje de correo electrónico y copie el código de seguridad de un solo uso que contiene.
7. Vuelva a Kaspersky Account y pegue el código en el campo de entrada.
8. Si ha configurado una pregunta secreta, respóndala.

   Si configura la verificación en dos pasos, introduzca el código de seguridad de uso único que ha recibido por SMS o que generó en la app de autenticación (según el método de verificación en dos pasos que haya configurado).
9. En la ventana que se abre, escriba una nueva contraseña.
10. Haga clic en **Guardar**.

    Se guardará la nueva contraseña para iniciar sesión en Kaspersky Security Center Cloud Console.

Si no ha recibido un mensaje de correo electrónico, compruebe la dirección introducida, su carpeta de correo no deseado e inténtelo nuevamente. Si no recibe un mensaje después de intentarlo nuevamente, es probable que la dirección de correo electrónico especificada no esté registrada en el sitio web. Póngase en contacto con el soporte técnico de Kaspersky.

Modificación de la configuración de una cuenta en Kaspersky Security Center Cloud Console

En esta sección, se proporcionan instrucciones para modificar y eliminar una cuenta en Kaspersky Security Center Cloud Console.

Cambiar una dirección de correo electrónico

Para cambiar su dirección de correo electrónico en la configuración de su cuenta en Kaspersky Security Center Cloud Console:

1. En Kaspersky Security Center Cloud Console, haga clic en el vínculo con el nombre de su cuenta y seleccione **Administrar cuenta de usuario**.

   Se abre la ventana **Mi perfil** del portal de Kaspersky Account.

2. Haga clic en el enlace **Cambiar su dirección de correo electrónico** (consulte la figura a continuación).

Cambiar la dirección de correo electrónico en la configuración de una cuenta en Kaspersky Security Center Cloud Console

3. En el campo de entrada **Dirección de correo electrónico nueva**, introduzca su nueva dirección de correo electrónico.

   Escriba la dirección con cuidado. Si introduce una dirección no válida, no podrá acceder a su cuenta ni utilizar Kaspersky Security Center Cloud Console.

4. Haga clic en el botón **Siguiente**.

5. En la ventana **Introducir su contraseña actual**, introduzca la contraseña de su cuenta en Kaspersky Security Center Cloud Console y haga clic en el botón **Continuar**.

6. Un mensaje de Kaspersky se envía a la dirección de correo electrónico que especificó. El mensaje contiene un código de seguridad de un solo uso.

   Abra el mensaje de correo electrónico y copie el código de seguridad de un solo uso que contiene.

7. Vuelva a Kaspersky Account y pegue el código en el campo de entrada.

8. Vuelva a Kaspersky Security Center Cloud Console haciendo clic en el enlace **Volver a Kaspersky Security Center Cloud Console** o salga del portal haciendo clic en el enlace **Cuenta → Cerrar sesión**.

Su dirección de correo electrónico se cambió en la configuración de la cuenta de Kaspersky Security Center Cloud Console y en la configuración de la cuenta de My Kaspersky. Se enviará un mensaje a su nueva dirección de correo electrónico para notificarle que ha cambiado la dirección de correo electrónico para acceder a su cuenta de usuario. La siguiente vez que inicie sesión en Kaspersky Security Center Cloud Console, tendrá que especificar su nueva dirección de correo electrónico.

Cambiar una contraseña

Para cambiar la contraseña en la configuración de su cuenta en Kaspersky Security Center Cloud Console:

1. En Kaspersky Security Center Cloud Console, haga clic en el vínculo con el nombre de su cuenta y seleccione **Administrar cuenta de usuario**.

   Se abre la ventana **Mi perfil** del portal de Kaspersky Account.

2. Haga clic en el enlace **Cambiar contraseña** (consulte la figura a continuación).

Cambiar la contraseña de la cuenta en Kaspersky Security Center Cloud Console

3. En el campo de entrada **Contraseña**, introduzca su nueva contraseña.

   Debajo del campo de entrada, se muestran los requisitos para la contraseña. Hasta que no cumpla con los requisitos, no podrá guardar la contraseña nueva.

4. Haga clic en el botón **Guardar**.

5. En la ventana **Introducir su contraseña actual**, introduzca la contraseña de su cuenta en Kaspersky Security Center Cloud Console y haga clic en el botón **Continuar**.

6. Seleccione o borre la casilla de verificación **Solicitar automáticamente el cambio de contraseña cada 180 días**.

   De forma predeterminada, esta casilla de verificación está seleccionada.

7. Vuelva a Kaspersky Security Center Cloud Console haciendo clic en el enlace **Volver a Kaspersky Security Center Cloud Console** o salga del portal haciendo clic en el enlace **Cuenta → Cerrar sesión**.

Su contraseña se ha cambiado. Tendrá que introducir la nueva contraseña al iniciar sesión en Kaspersky Security Center Cloud Console y al iniciar sesión en My Kaspersky.

Uso de la verificación de dos pasos

En esta sección se describe la verificación de dos pasos, que puede ayudarle a mejorar la seguridad de su cuenta en Kaspersky Security Center Cloud Console.

Acerca de la verificación de dos pasos

La verificación de dos pasos puede ayudarle a mejorar la seguridad de su cuenta en Kaspersky Security Center Cloud Console. Cuando esta función está activada, cada vez que inicie sesión en Kaspersky Security Center Cloud Console con su dirección de correo electrónico y contraseña, introducirá un código de seguridad adicional de uso único. Con la verificación de dos pasos, los delincuentes no pueden iniciar sesión en su cuenta si roban o adivinan su contraseña, ya que también deberían tener acceso a su teléfono móvil. Además, cuando se activa la verificación en dos pasos, debe introducir un código de seguridad adicional de uso único si olvida su contraseña.

Después de configurar la verificación en dos pasos, es responsable de preservar la seguridad física de su teléfono y de mantener el acceso a su número de teléfono.

Puede obtener un código de seguridad de uso único de una de las siguientes maneras:

- Se envía un código de seguridad por SMS al número de su teléfono móvil.

  En este caso, si pierde el acceso a su teléfono móvil, no podrá iniciar sesión en su cuenta en Kaspersky Security Center Cloud Console hasta que restaure el acceso a su número de teléfono.

- Se genera un código de seguridad en una aplicación autenticadora que se instala en su teléfono móvil.

  Le recomendamos que configure la verificación en dos pasos con una aplicación de autenticación. En este caso, puede iniciar sesión en su cuenta aunque su teléfono móvil no esté conectado a Internet o a una red móvil.

  Solo hemos comprobado la compatibilidad de Google Authenticator y Microsoft Authenticator con Kaspersky Security Center Cloud Console, y estas aplicaciones eran gratuitas al momento de realizar la prueba. Las interfaces de estas aplicaciones pueden no estar disponibles en su idioma. Compruebe además el cumplimiento del RGPD y las políticas de privacidad de las aplicaciones antes de usarlas. Kaspersky no está patrocinado, respaldado ni afiliado de ninguna otra manera a los propietarios de estas aplicaciones.

  > Microsoft Authenticator solo se puede instalar en dispositivos móviles.

  También le recomendamos que instale una aplicación de autenticación en otro dispositivo, además de su teléfono móvil. Esto le permitirá iniciar sesión en su cuenta incluso si le robaran su teléfono móvil o lo perdiera.

En este caso, si pierde el acceso a su teléfono móvil y no tiene una aplicación de autenticación en otro dispositivo, no podrá iniciar sesión en su cuenta en Kaspersky Security Center Cloud Console hasta que restaure el acceso a su número de teléfono. Después de eso, use el código de seguridad que se envía por SMS.

Si previamente ha configurado una pregunta secreta para restaurar su contraseña en caso de que la pierda, la función de la pregunta de seguridad se desactivará de forma permanente si configura la verificación en dos pasos.

Escenario: configuración de la verificación de dos pasos

La verificación de dos pasos puede ayudarle a mejorar la seguridad de su cuenta en Kaspersky Security Center Cloud Console. Después de completar el escenario en esta sección, se configurará la verificación de dos pasos de su cuenta.

El escenario se divide en etapas:

1. **Añadir su número de teléfono**

   En esta etapa, debe configurar la verificación en dos pasos por SMS.

2. **Instalar y configurar una aplicación de autenticación**

   Instale y configure una aplicación de autenticación.

   Le recomendamos que configure la verificación en dos pasos con una aplicación de autenticación. En este caso, puede iniciar sesión en su cuenta aunque su teléfono móvil no esté conectado a Internet o a una red móvil.

   También le recomendamos que instale una aplicación de autenticación en otro dispositivo, además de su teléfono móvil. Esto le permitirá iniciar sesión en su cuenta aunque pierda su teléfono o se lo roben.

3. **Cambiar su número de teléfono**

   Si es necesario, puede cambiar el número de teléfono que utiliza para la verificación en dos pasos.

Configuración de la verificación de dos pasos por SMS

Para configurar la verificación en dos pasos por SMS:

1. En Kaspersky Security Center Cloud Console, haga clic en el vínculo con el nombre de su cuenta y seleccione **Administrar cuenta de usuario**.

   Se abre la ventana **Mi perfil** del portal de Kaspersky Account.

2. Si la verificación en dos pasos está desactivada, active el conmutador **La verificación en dos pasos está desactivada**.

3. En la ventana **No se ha proporcionado ningún número de teléfono**, haga clic en el botón **Confirmar**.

4. En **Especificar el número del teléfono móvil**, especifique el número de teléfono móvil que desea utilizar en la verificación en dos pasos y haga clic en el botón **Proporcionar número de teléfono**.

   Puede usar el mismo número de teléfono para un máximo de cinco cuentas.

Se enviará un código de seguridad de 6 dígitos al número de teléfono especificado.

5. En **Ingrese el código de verificación que se envió a <número de teléfono>**, introduzca el código de seguridad recibido.

6. En la ventana **Introducir su contraseña actual**, introduzca la contraseña de su cuenta en Kaspersky Security Center Cloud Console y haga clic en el botón **Continuar**.

La verificación en dos pasos está configurada. Ahora, cada vez que inicie sesión con su dirección de correo electrónico y contraseña, o si olvida su contraseña, deberá introducir un código de seguridad de uso único que recibirá por SMS al número de teléfono especificado.

Ahora puede instalar y configurar una aplicación de autenticación, cambiar su número de teléfono o desactivar la verificación en dos pasos.

Configurar la verificación en dos pasos a través de una aplicación autenticadora

Las aplicaciones autenticadoras no pueden utilizarse como método de verificación independiente en Kaspersky Security Center Cloud Console. Primero debe configurar la verificación en dos pasos por SMS. Si desactiva la verificación en dos pasos a través de su número de teléfono móvil, la verificación a través de una aplicación de autenticación se desactiva automáticamente. Después de configurar tanto la verificación por SMS como a través de una aplicación, podrá seleccionar un método de verificación en la página de inicio de sesión o bien si olvida la contraseña.

Para configurar la verificación en dos pasos a través de una aplicación de autenticación:

1. Configure la verificación en dos pasos por SMS.

2. Descargue, instale y ejecute la aplicación autenticadora que desea usar.

   Solo hemos comprobado la compatibilidad de Google Authenticator y Microsoft Authenticator con Kaspersky Security Center Cloud Console, y estas aplicaciones eran gratuitas al momento de realizar la prueba. Las interfaces de estas aplicaciones pueden no estar disponibles en su idioma. Compruebe además el cumplimiento del RGPD y las políticas de privacidad de las aplicaciones antes de usarlas. Kaspersky no está patrocinado, respaldado ni afiliado de ninguna otra manera a los propietarios de estas aplicaciones.

   > Microsoft Authenticator solo se puede instalar en dispositivos móviles.

   Si lo desea, puede usar otras aplicaciones a su propio riesgo. La aplicación que use debe admitir códigos de seguridad de 6 dígitos.

   También le recomendamos que instale una aplicación de autenticación en otro dispositivo, además de su teléfono móvil. Esto le permitirá iniciar sesión en su cuenta incluso si le robaran su teléfono móvil o lo perdiera.

3. En Kaspersky Security Center Cloud Console, haga clic en el vínculo con el nombre de su cuenta y seleccione **Administrar cuenta de usuario**.

   Se abre la ventana **Mi perfil** del portal de Kaspersky Account.

4. Si la verificación en dos pasos está desactivada, active el conmutador **La verificación en dos pasos está desactivada**.

5. Active el conmutador **La app de autenticación está desactivada**.

   La página del portal muestra un código QR.

Si desea configurar la aplicación de autenticación en un dispositivo que no puede escanear códigos QR, haga clic en el enlace **No puedo escanearlo**. Se muestra una clave secreta de 16 caracteres.

6. En la aplicación de autenticación de cada dispositivo, escanee el código QR para crear una cuenta. Consulte la documentación de la aplicación para obtener más información.

   Si desea configurar la aplicación de autenticación en un dispositivo que no puede escanear códigos QR, cree una cuenta en la app de autenticación y luego introduzca la clave secreta que aparezca.

   Se genera un código de seguridad de 6 dígitos en sus aplicaciones de autenticación.

7. Verifique que los códigos de seguridad generados en las aplicaciones sean los mismos en cada dispositivo.

8. Vuelva al portal de Kaspersky Account y haga clic en el botón **Siguiente**.

9. Ingrese el código de seguridad generado.

10. En la ventana **Introducir su contraseña actual**, introduzca la contraseña de su cuenta en Kaspersky Security Center Cloud Console y haga clic en el botón **Continuar**.

La verificación de dos pasos a través de una aplicación autenticadora está configurada. Ahora, cada vez que inicie sesión con su dirección de correo electrónico y contraseña, o si olvida su contraseña, deberá introducir un código de seguridad de uso único que se genera en la aplicación de autenticación.

Ahora puede desactivar el uso de una aplicación de autenticación o desactivar por completo la verificación en dos pasos.

Cambio de su número de teléfono

Para cambiar el número de teléfono que se usa en la verificación en dos pasos por SMS:

1. En Kaspersky Security Center Cloud Console, haga clic en el vínculo con el nombre de su cuenta y seleccione **Administrar cuenta de usuario**.

   Se abre la ventana **Mi perfil** del portal de Kaspersky Account.

2. Si la verificación en dos pasos está desactivada, active el conmutador **La verificación en dos pasos está desactivada**.

3. En **Número de teléfono**, haga clic en el enlace **Cambiar el número de teléfono**.

4. En **Especificar el número del teléfono móvil**, especifique el nuevo número de teléfono móvil que desea utilizar en la verificación en dos pasos y haga clic en el botón **Proporcione su número de teléfono**.

   Se enviará un código de seguridad de 6 dígitos al número de teléfono especificado.

5. En **Ingrese el código de verificación que se envió a <número de teléfono>**, introduzca el código de seguridad recibido.

Se cambiará el número de su teléfono móvil. Ahora se enviarán códigos de seguridad de uso único al nuevo número de teléfono.

Desactivación de la verificación de dos pasos

Si ya no desea usar la verificación en dos pasos, puede desactivarla, como se describe en esta sección.

La desactivación de la verificación en dos pasos reducirá la seguridad de su cuenta. Le recomendamos que siga usando la verificación en dos pasos.

Si configura la verificación en dos pasos por SMS, puede desactivar la verificación en dos pasos. Si configura la verificación en dos pasos a través de una aplicación de autenticación, puede desactivar el uso de la aplicación o desactivar por completo la verificación en dos pasos.

Para deshabilitar el uso de la aplicación de autenticación, haga lo siguiente:

1. En Kaspersky Security Center Cloud Console, haga clic en el vínculo con el nombre de su cuenta y seleccione **Administrar cuenta de usuario**.

   Se abre la ventana **Mi perfil** del portal de Kaspersky Account.

2. Desactive el conmutador de la **App de autenticación**.

3. En la ventana de confirmación que se abre, haga clic en el botón **Confirmar**.

4. En la ventana **Introducir su contraseña actual**, introduzca la contraseña de su cuenta en Kaspersky Security Center Cloud Console y haga clic en el botón **Continuar**.

   Se desactivará el uso de una aplicación de autenticación. Se eliminará la configuración de la verificación en dos pasos a través de una aplicación de autenticación. Ahora puede eliminar cuentas en las aplicaciones autenticadoras.

   Más adelante, puede configurar la verificación en dos pasos a través de una aplicación de autenticación nuevamente.

Para desactivar por completo la verificación en dos pasos:

1. En Kaspersky Security Center Cloud Console, haga clic en el vínculo con el nombre de su cuenta y seleccione **Administrar cuenta de usuario**.

   Se abre la ventana **Mi perfil** del portal de Kaspersky Account.

2. Desactive el conmutador **La verificación en dos pasos está activada**.

3. En la ventana de confirmación que se abre, haga clic en el botón **Confirmar**.

4. En la ventana **Introducir su contraseña actual**, introduzca la contraseña de su cuenta en Kaspersky Security Center Cloud Console y haga clic en el botón **Continuar**.

   Se desactivará la verificación en dos pasos. Si ha utilizado la verificación en dos pasos a través de una aplicación de autenticación, se eliminará la configuración de la verificación en dos pasos. Ahora puede eliminar cuentas en las aplicaciones autenticadoras.

   Más adelante, puede configurar la verificación en dos pasos nuevamente.

Eliminación de una cuenta en Kaspersky Security Center Cloud Console

Si desea dejar de utilizar Kaspersky Security Center Cloud Console, puede eliminar su cuenta.

Al eliminar una cuenta, se pierden todos los datos asociados con esa cuenta.

Después de eliminar la cuenta, ya no podrá acceder a sus espacios de trabajo en Kaspersky Endpoint Security Cloud, Kaspersky Security for Microsoft Office 365 y Kaspersky Security Center Cloud Console. Si era el único administrador en un espacio de trabajo, el espacio de trabajo se eliminará debidamente. Además, perderá el acceso a su cuenta de My Kaspersky.

Para eliminar una cuenta en Kaspersky Security Center Cloud Console:

1. En Kaspersky Security Center Cloud Console, haga clic en el vínculo con el nombre de su cuenta y seleccione **Administrar cuenta de usuario**.

   Se abre la ventana **Mi perfil** del portal de Kaspersky Account.

2. Haga clic en el enlace **Cuenta** → **Eliminar**.

3. En la ventana **Eliminar su cuenta** que se abre, lea la información sobre las consecuencias de la eliminación de la cuenta y luego haga clic en el botón **Eliminar** para confirmar la eliminación de la cuenta.

4. En la ventana **Introducir su contraseña actual**, introduzca la contraseña de su cuenta en Kaspersky Security Center Cloud Console y haga clic en el botón **Continuar**.

Se elimina su cuenta.

Selección de los centros de datos usados para guardar información de Kaspersky Security Center Cloud Console

Se crea un espacio de trabajo para Kaspersky Security Center Cloud Console con servidores de una red de centros de datos globales en una plataforma de nube. La selección de los centros de datos que alojarán un espacio de trabajo depende del país que haya especificado al registrar la empresa en Kaspersky Security Center Cloud Console (consulte la tabla a continuación). Los paquetes de distribución de las aplicaciones de seguridad están alojados en los mismos servidores que los espacios de trabajo.

Correspondencia de la ubicación de la empresa con una región del centro de datos

El país donde se encuentra la empresa	Región del centro de datos
Argentina	Brasil
Bolivia	Brasil
Brasil	Brasil
Chile	Brasil
Colombia	Brasil
Ecuador	Brasil
Guyana	Brasil
Perú	Brasil
Paraguay	Brasil
Surinam	Brasil
Uruguay	Brasil
Venezuela	Brasil
Antigua y Barbuda	México o Brasil

Anguila	México o Brasil
Aruba	México o Brasil
Barbados	México o Brasil
San Bartolomé	México o Brasil
Bonaire, San Eustaquio y Saba	México o Brasil
Belice	México o Brasil
Costa Rica	México o Brasil
Cuba	México o Brasil
Curazao	México o Brasil
Dominica	México o Brasil
República Dominicana	México o Brasil
Granada	México o Brasil
Guadalupe	México o Brasil
Guatemala	México o Brasil
Honduras	México o Brasil
Haití	México o Brasil
Jamaica	México o Brasil
San Cristóbal y Nieves	México o Brasil
Islas Caimán	México o Brasil
Santa Lucía	México o Brasil
San Martín	México o Brasil
Martinica	México o Brasil
Montserrat	México o Brasil
Nicaragua	México o Brasil
Panamá	México o Brasil
Sint Maarten	México o Brasil
Trinidad y Tobago	México o Brasil
San Vicente y las Granadinas	México o Brasil
Islas Vírgenes Británicas	México o Brasil
Japón	México o Irlanda
Canadá (Nuevo Brunswick)	México o Brasil
Canadá (Terranova y Labrador)	México o Brasil
Canadá (Nueva Escocia)	México o Brasil
Canadá (Ontario)	México o Brasil
Canadá (la Isla del Príncipe Eduardo)	México o Brasil
Canadá (Quebec)	México o Brasil
Albania	Irlanda
Bosnia-Herzegovina	Irlanda
Bulgaria	Irlanda
Bielorrusia	Irlanda
República Checa	Irlanda
Dinamarca	Irlanda

Estonia	Irlanda
Finlandia	Irlanda
Reino Unido	Irlanda
Groenlandia	Irlanda
Grecia	Irlanda
Croacia	Irlanda
Hungría	Irlanda
Irlanda	Irlanda
Islandia	Irlanda
Kirguistán	Irlanda
Kazajistán	Irlanda
Lituania	Irlanda
Letonia	Irlanda
Moldavia	Irlanda
Montenegro	Irlanda
Macedonia	Irlanda
Mongolia	Irlanda
Noruega	Irlanda
Polonia	Irlanda
Rumanía	Irlanda
Serbia	Irlanda
Federación de Rusia	Irlanda
Suecia	Irlanda
Eslovenia	Irlanda
Eslovaquia	Irlanda
Tayikistán	Irlanda
Turkmenistán	Irlanda
Uzbekistán	Irlanda
Canadá (Alberta)	México o Brasil
Canadá (Columbia Británica)	México o Brasil
Canadá (Manitoba)	México o Brasil
Canadá (Territorios del Noroeste)	México o Brasil
Canadá (Nunavut)	México o Brasil
Canadá (Yukón)	México o Brasil
Canadá (Saskatchewan)	México o Brasil
México	México o Brasil
Otros países	Irlanda

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 Cloud Console 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 de dispositivos cliente, ya que el Agente de red establece una conexión TCP/UDP con el servidor DNS. Si Kaspersky Security Center Cloud Console utiliza un servidor DNS público, el procesamiento de datos se rige por la política de privacidad del servicio correspondiente.

Escenario: creación de una jerarquía de servidores de administración administrados a través de Kaspersky Security Center Cloud Console

Este escenario describe las acciones que debe realizar para crear una jerarquía de Servidores de administración administrados a través de Kaspersky Security Center Cloud Console, que asume el rol de Servidor de administración principal. Esta jerarquía se puede usar posteriormente para la migración de dispositivos y objetos administrados de Kaspersky Security Center a Kaspersky Security Center Cloud Console, así como para la administración de Servidores de administración secundarios y dispositivos a través de Kaspersky Security Center Cloud Console.

Kaspersky Security Center Cloud Console solo puede actuar como Servidor de administración principal, mientras que los Servidores de administración que se ejecutan de forma local solo pueden actuar como Servidores de administración secundarios. No hay otros esquemas jerárquicos disponibles.

Requisitos previos

Antes de comenzar, asegúrese de que se cumplan los siguientes requisitos previos:

- Actualización del Servidor de administración que se ejecuta en las instalaciones, hasta la versión 12 o posteriores.
- Instalación de Kaspersky Security Center Web Console en el Servidor de administración que se ejecuta de forma local.
- Instalar los complementos web para las aplicaciones que va a administrar a través de Kaspersky Security Center Cloud Console.
- Actualizar las aplicaciones administradas a versiones compatibles con Kaspersky Security Center Cloud Console.
- Asegurarse de que la descarga de actualizaciones en la tarea de repositorio del Servidor de administración cuando este se ejecuta de forma local no tenga el Servidor de administración principal asignado como origen de actualizaciones; modificar la configuración de la tarea en consecuencia, si es necesario.

Después de crear la jerarquía, las directivas y tareas que son efectivas en Kaspersky Security Center Cloud Console se aplican en el Servidor de administración secundario, y reemplazan sus directivas y tareas existentes. Si no desea que esto pase, elimine todas las directivas y tareas de Kaspersky Security Center Cloud Console antes de crear la jerarquía. De manera alternativa, puede cambiar el estado de cada directiva de Kaspersky Security Center Cloud Console a **Inactiva** en su configuración y desactivar la opción **Distribuir a Servidores de administración secundarios y virtuales** en la configuración de cada tarea de Kaspersky Security Center Cloud Console.

Puede eliminar su jerarquía de Servidores de administración en cualquier momento, si es necesario.

Etapas de creación de una jerarquía

El escenario básico se aplica un Servidor de administración secundario al que no se puede acceder a través de Internet. Sin embargo, el conjunto de acciones dentro de algunos de los pasos descritos a continuación podría variar si es posible acceder al Servidor de administración secundario a través de Internet. Además, algunos de los pasos deben omitirse en este caso.

La creación de una jerarquía de Servidores de administración comprende las siguientes etapas:

1. **Recuperación del certificado del Servidor de administración secundario**

   Si se puede acceder al Servidor de administración secundario a través de Internet, omita este paso.

   En Kaspersky Security Center Web Console que se ejecuta de forma local, abra las propiedades del Servidor de administración y, en la pestaña **General**, abra la sección **General**. Haga click en el enlace **Ver certificado del Servidor de administración** El archivo del certificado, en formato CER, se guarda automáticamente en la carpeta especificada en la configuración de su navegador.

2. **Recuperación de la configuración de conexión y los certificados de Kaspersky Security Center Cloud Console**

   Si se puede acceder al Servidor de administración secundario a través de Internet, omita este paso.

   En Kaspersky Security Center Cloud Console, abra las propiedades del Servidor de administración y, en la pestaña **General**, abra la sección **Jerarquía de Servidores de administración**. Se muestran las siguientes configuraciones de conexión:

   - Dirección de HDS

     Muestra la dirección web que se utiliza para la conexión con el servicio de detección hospedado (HDS).

   - Puerto HDS

     Muestra el número del puerto utilizado para la conexión a HDS.

   La sección también contiene dos enlaces:

   - Ver certificado del Servidor de administración

     Al hacer clic en este enlace, se inicia la descarga de la clave pública del certificado de instancia de Kaspersky Security Center Cloud Console.

   - Certificado de CA raíz de HDS

     Al hacer clic en este enlace, se inicia la descarga del archivo en formato .pem que contiene una lista de certificados raíz expedidos por Autoridades de certificación (CA). Este archivo está diseñado para que lo use el Servidor de administración secundario: es necesario para verificar el certificado HDS.

Copie la configuración de conexión manualmente, utilizando el portapapeles o cualquier otra forma adecuada, y guárdela en un archivo con cualquier formato conveniente. Haga clic en el enlace **Ver certificado del Servidor de administración** y espere hasta que se descargue el archivo del certificado. Haga clic en el enlace **Certificado de CA raíz de HDS** y espere a que se descargue el archivo con la lista de certificados raíz de confianza emitidos por las Autoridades de certificación. Ambos archivos se guardan en la carpeta especificada en la configuración de su navegador.

3 Selección del Servidor de administración secundario para la conexión

En las propiedades del Servidor de administración, diríjase a la pestaña **Servidores de administración**. En la jerarquía de grupos de administración, seleccione la casilla de verificación junto al grupo de administración que desea que contenga el Servidor de administración secundario con todos sus dispositivos administrados. Haga click en el botón **Conectar Servidor de administración secundario**

En la página que se abre, en el campo **Nombre a mostrar del Servidor de administración secundario**, especifique el nombre con el que se debe mostrar el Servidor de administración secundario en la jerarquía. Se usa solo para su conveniencia y, por lo tanto, puede diferir del nombre real del Servidor de administración secundario, si es necesario. Haga clic en **Siguiente**.

Si se puede acceder al Servidor de administración secundario a través de Internet, también debe especificar la dirección del Servidor de administración secundario en el campo **Dirección del Servidor de administración secundario (opcional)**.

En la página siguiente, haga clic en el botón **Examinar** y especifique el archivo .pem que guardó del Servidor de administración secundario. Haga clic en **Siguiente**.

4 Activación y configuración del servidor proxy

Las acciones descritas en este paso son opcionales. Realícelas solo si su conexión exige el uso de un servidor proxy.

Haga clic en **Siguiente**. En la página **Configuración de conexiones y autenticación**, puede activar y configurar el uso del servidor proxy, si es necesario. Selecciona la casilla de verificación **Usar servidor proxy** y especifique la siguiente configuración de proxy:

- Dirección del servidor proxy

  La dirección del servidor proxy.

- Nombre de usuario

  El nombre de usuario para iniciar sesión en el servidor proxy.

- Contraseña

  La contraseña para iniciar sesión en el servidor proxy.

5 Especificación de la configuración de autenticación y adición del Servidor de administración secundario a la jerarquía

Haga clic en **Siguiente**. En la página **Credenciales del Servidor de administración secundario**, especifique los siguientes ajustes:

- Nombre de usuario

El nombre de usuario con el que inicia sesión en el Servidor de administración secundario.

- Contraseña

  La contraseña utilizada para iniciar sesión en el Servidor de administración secundario.

Hacer clic **Siguiente** y espere hasta que el Servidor de administración secundario aparezca en la jerarquía.

Si se puede acceder al Servidor de administración secundario a través de Internet, se conecta al Servidor de administración principal.

Si se puede acceder al Servidor de administración secundario a través de Internet y la conexión entre los dos Servidores de administración se establece correctamente, omita todos los pasos adicionales.

Si no se puede acceder al Servidor de administración secundario a través de Internet, se hace visible, pero debe realizar acciones adicionales en el Servidor de administración secundario para poder controlarlo.

6. **Configuración de la conexión en Kaspersky Security Center Web Console que se ejecuta de forma local**

   En Kaspersky Security Center Web Console que se ejecuta de forma local, abra las propiedades del Servidor de administración y, en la pestaña **General**, abra la sección **Jerarquía de Servidores de administración**. Marque la casilla **Este Servidor de administración es secundario en la jerarquía**. En la lista **Datos del Servidor de administración principal**, seleccione la opción **Kaspersky Security Center Cloud Console**.

   Kaspersky Security Center Web Console verifica si el Servidor de administración principal está especificado como el origen de actualizaciones en la tarea *Descargar actualizaciones del repositorio del Servidor de administración*. Si el Servidor de administración principal se especifica como el origen de actualizaciones, obtendrá el mensaje de advertencia correspondiente y un enlace a la configuración de la tarea. Puede modificar la configuración y luego volver a la creación de la jerarquía o puede omitir esta acción y continuar con la creación de la jerarquía.

   En el grupo **Configuración para establecer la conexión entre los Servidores de administración principal y secundario**, especifique la siguiente configuración:

   - Dirección del Servidor HDS (del Servidor de administración principal en Cloud Console)

     Ingrese la dirección del servidor HDS en formato de nombre de dominio completo (FQDN), que ha copiado y guardado de las propiedades del Servidor de administración en Kaspersky Security Center Cloud Console.

   - Puertos del servidor HDS

     Introduzca los números de los puertos del servidor HDS, que ha copiado y guardado de las propiedades del Servidor de administración en Kaspersky Security Center Cloud Console.

7. **Añadir certificados al Servidor de administración secundario**

   Haga clic en el botón **Especificar el certificado del Servidor de administración principal** y especifique el archivo de certificado que guardó desde las propiedades del Servidor de administración en Kaspersky Security Center Cloud Console.

   Haga clic en el botón **Especificar certificados del servicio Hosted Discovery Service** y especifique el archivo .pem que guardó de las propiedades del Servidor de administración en Kaspersky Security Center Cloud Console.

Si ha activado el uso del servidor proxy al conectar el Servidor de administración secundario en Kaspersky Security Center Cloud Console, seleccione la casilla de verificación **Usar servidor proxy** y especifique la misma configuración de proxy que en Kaspersky Security Center Cloud Console.

También puede seleccionar la casilla de verificación **Conectar Servidor de administración principal a Servidor de administración secundario en DMZ** si el Servidor de administración secundario está en una zona desmilitarizada (DMZ).

El Servidor de administración secundario se conecta al Servidor de administración principal.

Resultados

Al realizar los pasos anteriores, puede asegurarse de que la jerarquía se haya creado correctamente:

- Las directivas activas del Servidor de administración principal entran en vigencia en el Servidor de administración secundario. Las tareas del Servidor de administración principal se distribuyen al Servidor de administración secundario. Si la opción **Distribuir a Servidores de administración secundarios y virtuales** está activada en la configuración de una tarea de grupo, cada una de esas tareas también se distribuye al Servidor de administración secundario.

- Los valores de la directiva que están bloqueados para evitar cambios en el Servidor de administración principal se muestran como bloqueados para realizar cambios en todas las directivas en el Servidor de administración secundario.

- Las directivas aplicadas por el Servidor de administración principal se muestran en la lista de directivas del Servidor de administración secundario (**Activos (dispositivos)** → **Directivas y perfiles**).

- Las tareas de grupo distribuidas por el Servidor de administración principal se muestran en la lista de tareas del Servidor de administración secundario (**Activos (dispositivos)** → **Tareas**).

- Las directivas y tareas creadas en el Servidor de administración principal no se pueden modificar en el Servidor de administración secundario.

- En Kaspersky Security Center Cloud Console, en la estructura de los grupos de administración, el Servidor de administración secundario se muestra dentro del grupo que seleccionó al agregar este Servidor de administración.

Migración a Kaspersky Security Center Cloud Console

Esta sección describe el proceso de migración a Kaspersky Security Center Cloud Console desde:

- Kaspersky Security Center Web Console versión 12 (o posterior) que se ejecuta de manera local.
- Pro View.

> La migración desde Pro View solo está disponible si tiene una licencia de Kaspersky Next.

Acerca de la migración desde Kaspersky Security Center Web Console

Esta sección describe el proceso de migración desde una instancia local de Kaspersky Security Center Web Console versión 12 (o posterior) a Kaspersky Security Center Cloud Console.

Métodos de migración a Kaspersky Security Center Cloud Console

Al usar la función de migración, puede transferir los dispositivos de red administrados por Kaspersky Security Center y ponerlos bajo la administración de Kaspersky Security Center Cloud Console. Sus dispositivos administrados migrarán sin perder sus principales ajustes, como la pertenencia a grupos de administración, así como los objetos esenciales, como directivas y tareas, relacionados con las aplicaciones administradas.

Puede elegir cualquiera de los dos métodos disponibles para migrar sus Servidores de administración a Kaspersky Security Center Cloud Console:

- Migración sin una jerarquía de Servidores de administración:
  - Permite transferir dispositivos administrados y objetos relacionados a Kaspersky Security Center Cloud Console, incluso si el Servidor de administración local no es secundario con respecto a Kaspersky Security Center Cloud Console.
  - Puede requerir la transferencia de archivos (en una unidad extraíble, por correo electrónico, a través de carpetas compartidas o de cualquier otra manera conveniente) si Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console están abiertos en diferentes dispositivos físicos.

  > También puede realizar migración con Servidores de administración virtuales si su red los incluye.

- Migración utilizando una jerarquía de Servidores de administración:
  - Permite la transferencia de dispositivos administrados y objetos relacionados a Kaspersky Security Center Cloud Console utilizando solo la interfaz de Kaspersky Security Center Cloud Console, por lo que no es necesaria la transferencia física de archivos.
  - Requiere que el Servidor de administración que se ejecuta localmente actúe como secundario de Kaspersky Security Center Cloud Console. Puede crear esa jerarquía antes de comenzar la migración.

El cifrado de disco completo de Kaspersky Security Center Cloud Console solo admite BitLocker.

Escenario: Migración sin una jerarquía de Servidores de administración

En esta sección, se describe la migración de los dispositivos administrados y los objetos relacionados (como directivas, tareas e informes) de Kaspersky Security Center Web Console local a Kaspersky Security Center Cloud Console. Puede incluir un solo grupo de administración en la cobertura de la migración para restaurar el mismo grupo de administración en Kaspersky Security Center Cloud Console.

Este grupo debe contener los dispositivos administrados de un solo sistema operativo. Si su red incluye los dispositivos de diferentes sistemas operativos o distribuciones de Linux, asígnelos a diferentes grupos de administración y migre cada grupo por separado.

Una vez finalizada la migración, todos los Agentes de red dentro de la cobertura de la migración se actualizan y se administran a través de Kaspersky Security Center Cloud Console.

Los pasos enumerados en esta sección cubren el proceso de migración realizado cuando no existe una jerarquía de Servidores de administración, es decir, no se ha establecido una conexión entre Kaspersky Security Center Cloud Console y la instancia local de Kaspersky Security Center Web Console.

Requisitos previos

Antes de comenzar, haga lo siguiente:

- Actualización del Servidor de administración que se ejecuta en las instalaciones, hasta la versión 14.2 o posteriores.
- Instale Kaspersky Security Center Web Console versión 12.1 o posterior.
- Actualice el Agente de red en los dispositivos administrados a la versión 12 o posterior.
- En dispositivos Windows, utilice el Agente de red sin una contraseña de desinstalación.

  Si ya se ha establecido la contraseña, realice una de las siguientes acciones en Kaspersky Security Center Web Console:

  - Desactive la opción **Utilizar contraseña de desinstalación** en la Network Agent policy settings.
  - Desinstale el Agente de red de forma remota mediante la tarea *Desinstalar aplicación en remoto*. En el campo **Aplicación que se va a desinstalar** de la tarea, seleccione **Agente de red de Kaspersky Security Center**. No olvide introducir la contraseña de desinstalación.
- Actualice las aplicaciones administradas a versiones compatibles con Kaspersky Security Center Cloud Console.
- Asegúrese de tener directivas para las últimas versiones de las aplicaciones administradas. Si sus directivas están desactualizadas, cree directivas nuevas para las versiones compatibles con Kaspersky Security Center Cloud Console.
- Para utilizar directivas reales, actualice los complementos web para las aplicaciones que desea administrar a través de Kaspersky Security Center Cloud Console.

- Desinstalar Aplicaciones Kaspersky desde dispositivos administrados si estas aplicaciones no son compatibles con Kaspersky Security Center Cloud Console.

- Descifre todos los datos (a nivel de disco o de archivo) que Kaspersky Endpoint Security para Windows cifró en los dispositivos administrados que ejecutan el sistema operativo Windows y desactive la función de cifrado en los dispositivos administrados a través de la directiva de la aplicación o de forma local. Para obtener más información, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

  Si el dispositivo Windows aún almacena archivos o carpetas cifrados a través de Kaspersky Endpoint Security para Windows, la actualización del Agente de red se cancelará durante el proceso de migración. Una notificación le pedirá que descifre todos los datos en el dispositivo y que desactive la función de cifrado.

Kaspersky Security Center Cloud Console permite que un Servidor de administración administre un máximo de 25 000 dispositivos administrados.

Etapas de la migración

La migración a Kaspersky Security Center Cloud Console comprende las siguientes etapas:

1. **Planificación de la cobertura de la migración y comprobación de los requisitos previos**

   Estime la cobertura del proceso de migración, es decir, revise el grupo de administración a exportar, y evalúe la cantidad de dispositivos administrados en él. Además, asegúrese de que todas las actividades enumeradas como requisitos previos de migración se hayan completado correctamente.

2. **Exportación de dispositivos administrados, objetos y configuraciones administradas desde Kaspersky Security Center Web Console**

   Utilice el Asistente de migración de ejecución local de Kaspersky Security Center Web Console para exportar los dispositivos administrados junto con los objetos.

   El tamaño máximo del archivo de exportación es de 4 GB.

3. **Importación del archivo de exportación en Kaspersky Security Center Cloud Console**

   Transfiera la información sobre sus dispositivos administrados y objetos a Kaspersky Security Center Cloud Console. A tal efecto, use el Asistente de migración de Kaspersky Security Center Cloud Console para importar el archivo de exportación y crear un paquete de instalación independiente del Agente de red.

4. **Reinstalación del Agente de red en los dispositivos administrados**

   Vuelva al Asistente de migración en Kaspersky Security Center Web Console que se ejecuta de forma local para crear una tarea de instalación remota. Podrá utilizar esta tarea (inmediatamente o más tarde) para volver a instalar el Agente de red en sus dispositivos administrados y completar el proceso de migración.

Resultados

Al finalizar la migración, puede asegurarse de que se haya realizado correctamente:

- El Agente de red se reinstaló en todos los dispositivos administrados.

- Todos los dispositivos se administran a través de Kaspersky Security Center Cloud Console.

- Se conservan todas las configuraciones de objetos que se utilizaban antes de la migración

Asistente de migración

Esta sección proporciona información sobre el Asistente de migración en Kaspersky Security Center Cloud Console y Kaspersky Security Center Web Console versión 12 o posterior.

Paso 1. Exportación de dispositivos administrados, objetos y configuraciones administradas desde Kaspersky Security Center Web Console

La migración de dispositivos administrados desde Kaspersky Security Center Web Console hasta Kaspersky Security Center Cloud Console requiere que primero cree un archivo de exportación que contenga información sobre la jerarquía de grupos de administración que están en su Servidor de administración local actual. El archivo de exportación también debe contener información sobre los objetos y sus ajustes. El archivo de exportación se utilizará para la importación posterior a Kaspersky Security Center Cloud Console.

El tamaño máximo del archivo de exportación es de 4 GB.

Para exportar objetos y su configuración desde Kaspersky Security Center Web Console, siga estos pasos:

1. En el menú principal de Kaspersky Security Center Web Console, vaya a **Operaciones** → **Migración**.
2. En la página de bienvenida del Asistente de migración, haga clic en **Siguiente**. Se abre la página **Dispositivos administrados para exportar** que muestra toda la jerarquía de grupos de administración del Servidor de administración correspondiente.
3. En la página **Dispositivos administrados para exportar**, haga clic en el icono de flecha (>) junto al lado del nombre de grupo **Dispositivos administrados** para expandir la jerarquía de los grupos de administración. Seleccione el grupo de administración que desea exportar.

   Después de la migración desde Kaspersky Security Center en las instalaciones hacia Kaspersky Security Center Cloud Console para dos grupos de administración, las tareas de instalación remota de estos grupos aparecen con el mismo nombre.

4. Seleccione las aplicaciones administradas cuyas directivas y tareas deben transferirse a Kaspersky Security Center Cloud Console junto con los objetos de grupo. Para seleccionar las aplicaciones administradas cuyos objetos se exportarán, seleccione las casillas de verificación junto a sus nombres en la lista.

   A pesar de que el Servidor de administración de Kaspersky Security Center se encuentra en la lista, al seleccionar la casilla de verificación correspondiente no se exportan sus directivas.

   Para asegurarse de que las aplicaciones administradas sean compatibles con Kaspersky Security Center Cloud Console, haga clic en el enlace correspondiente. Este le redirigirá al tema de Ayuda en línea que contiene la lista de aplicaciones administradas por Kaspersky Security Center Cloud Console.

Si selecciona aplicaciones que no sean compatibles con Kaspersky Security Center Cloud Console, las directivas y las tareas de estas aplicaciones se exportarán de todos modos y luego se importarán. No obstante, no podrá administrarlas en Kaspersky Security Center Cloud Console debido a la falta de disponibilidad de complementos dedicados.

5. Vea la lista de objetos del grupo exportados de forma predeterminada y especifique objetos que no sean del grupo para exportarlos junto con el grupo de administración seleccionado, de ser necesario. Para configurar la cobertura de la exportación, incluya o excluya varios objetos, como tareas globales, selecciones de dispositivos personalizados, informes, funciones personalizadas, usuarios internos y grupos de seguridad, y categorías de aplicaciones personalizadas. Esta página incluye las siguientes secciones:

   - **Tareas globales**

     La lista de tareas globales de las aplicaciones administradas, así como las tareas globales del Agente de red.

     Si una tarea global seleccionada se aplica a una selección de objeto específica, esta selección también se exportará.

     Aunque las tareas globales del Servidor de administración se encuentran en la lista, no puede exportarlas. Seleccionar dichas tareas no afecta el alcance de la exportación. Las tareas de instalación remota también quedan fuera del alcance de la exportación, porque sus respectivos paquetes de instalación no se pueden exportar.

   - **Selecciones de dispositivos**

     La lista de selecciones de dispositivos personalizadas.

   - **Informes**

     La lista editable de instancias de informes que se exportarán.

     Si un informe seleccionado se aplica a una selección de objeto específica, esta selección también se exportará.

     Kaspersky Security Center Cloud Console tiene el mismo conjunto de plantillas de informes que Kaspersky Security Center Web Console, por lo que puede seleccionar para exportar solo los informes que creó manualmente o volvió a configurar.

   - **Objetos de grupo**

La lista de objetos de grupo que se exportarán de forma predeterminada. Los siguientes objetos relacionados con el grupo de administración seleccionado se exportarán de forma predeterminada en su totalidad:

- La estructura del grupo de administración, es decir, todos los subgrupos del grupo de administración seleccionado
- Los dispositivos incluidos en los grupos de administración que se exportarán
- Las etiquetas asignadas a los dispositivos que se exportarán.

  Si se creó una etiqueta en Kaspersky Security Center Web Console, pero nunca se la asignó a ningún dispositivo, entonces no se exportará. Las reglas del etiquetado automático tampoco se exportarán.

- Las directivas de grupo de las aplicaciones administradas que se han seleccionado

  Las directivas del Servidor de administración y las directivas del Agente de red no se exportan.

- Tareas de grupo de las aplicaciones administradas que han sido seleccionadas y tareas de grupo del Agente de Red.

  Las tareas del Servidor de administración no se exportan.

También puede evitar que se exporten determinados tipos de objetos que no sean de grupo:

- Para cancelar la exportación de funciones personalizadas (es decir, aquellas creadas solo por el usuario), seleccione la casilla de verificación **Excluir funciones personalizadas de la exportación**.
- Para cancelar la exportación de usuarios internos y grupos de seguridad, seleccione la casilla de verificación **Excluir usuarios internos y grupos de seguridad de la exportación**.
- Para cancelar la exportación de categorías de aplicaciones personalizadas con contenido añadido manualmente, seleccione la casilla de verificación **Excluir categorías de aplicaciones personalizadas de la exportación**.

Si transfiere dispositivos de varios sistemas operativos a Kaspersky Security Center Cloud Console, los objetos que no sean de grupo solo se deben migrar una vez.

El Asistente de migración verifica el número total de dispositivos administrados que se incluyen en el grupo de administración seleccionado. Si este número supera los 10 000, aparece un mensaje de error. El botón **Siguiente** permanece no disponible (atenuado) hasta que el número de dispositivos administrados en el grupo de administración seleccionado cae dentro del límite.

6. Después de definir la cobertura de la migración, haga clic en **Siguiente** para comenzar el proceso de exportación. Se abre la página **Creando el archivo de exportación**, donde puede ver el progreso de la exportación para cada tipo de objeto que incluyó en la cobertura de la migración. 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 (✓). El proceso de exportación finaliza y el archivo de exportación se descarga automáticamente a

la ubicación de descarga predeterminada definida en la configuración de su navegador. El nombre del archivo de exportación aparece en la parte inferior de la ventana del navegador.

7. Cuando se muestre la página **La exportación se ha completado correctamente**, pase a la siguiente etapa que se ejecuta en Kaspersky Security Center Cloud Console.

Si utiliza Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console en diferentes dispositivos, deberá copiar el archivo de exportación a una unidad extraíble o elegir otras formas de transferir el archivo.

Paso 2. Importación del archivo de exportación en Kaspersky Security Center Cloud Console

Para transferir información exportada desde Kaspersky Security Center Web Console sobre dispositivos administrados, objetos y sus configuraciones, debe importarla a la aplicación de Kaspersky Security Center Cloud Console desplegada en su espacio de trabajo. Esto le permite crear un paquete de instalación independiente y utilizarlo para volver a instalar el Agente de red en sus dispositivos administrados.

Antes de iniciar el Asistente de migración en Kaspersky Security Center Cloud Console, asegúrese de que el idioma de localización actual sea el mismo que el idioma de Kaspersky Security Center Web Console durante el proceso de exportación. Cambie el idioma, si es necesario.

Si previamente completó el asistente de inicio rápido en el espacio de trabajo de Kaspersky Security Center Cloud Console, el grupo **Dispositivos administrados** incluye directivas y tareas creadas con la configuración predeterminada. Elimine estas directivas y tareas antes de importar las que exportó desde Kaspersky Security Center Web Console.

Para importar del archivo de exportación en Kaspersky Security Center Cloud Console:

1. En el menú principal de Kaspersky Security Center Cloud Console, vaya a **Operaciones** → **Migración**.

2. En la página de bienvenida del Asistente de migración, haga clic en **Importar**. En la ventana de Explorador de archivos que se abre, seleccione el archivo de exportación en la carpeta donde lo guardó y haga clic en **Abrir**. Espere a que el icono de actualización (🔄) junto al estado de carga del archivo se reemplace con la marca de verificación color verde (✓).

3. Haga clic en **Siguiente**. Se abre la siguiente página, que muestra toda la jerarquía de grupos de administración del Servidor de administración en Kaspersky Security Center Cloud Console.

4. Seleccione la casilla de verificación junto al grupo de administración de destino en el que se deben restaurar los objetos del grupo y haga clic en **Siguiente**. El Asistente de migración muestra una lista de los paquetes de instalación del Agente de red que están disponibles en Kaspersky Security Center Cloud Console.

5. Seleccione el paquete de instalación que contenga la versión relevante y la localización del Agente de red y haga clic en **Siguiente**.

Seleccione el paquete de instalación del Agente de red para Windows de Kaspersky solo si completó previamente el asistente de inicio rápido en el espacio de trabajo de Kaspersky Security Center Cloud Console y si realiza la migración de dispositivos Windows.

Espere a que el Asistente de migración cree un paquete de instalación independiente. El tamaño máximo de archivo del paquete de instalación independiente para el Agente de red es de 200 MB.

El archivo se descomprime y se descarga automáticamente en la ubicación de descarga predeterminada definida en la configuración de su navegador. Los objetos de grupo y los que no son de grupo se restauran al grupo de administración de destino.

Cuando termina la importación, la estructura exportada de los grupos de administración, incluidos los detalles de los dispositivos, 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 ha importado el grupo **Dispositivos administrados** por completo, le recomendamos que cambie el nombre del subgrupo recién importado para evitar confusiones:

a. Vaya a la sección **Jerarquía de grupos**.

b. Haga clic en el nombre del subgrupo en el árbol de los grupos.

c. En la ventana de propiedades que se abre, en el campo **Nombre**, introduzca un nombre diferente (por ejemplo, "Dispositivos migrados").

Le recomendamos que verifique que los objetos (directivas, tareas y dispositivos administrados) incluidos en el alcance de exportación se hayan importado de forma correcta en Kaspersky Security Center Cloud Console. Para ello, diríjase a la sección **Activos (dispositivos)** y compruebe que los objetos importados aparezcan en las listas en las subsecciones **Directivas y perfiles**, **Tareas** y **Dispositivos administrados**.

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. Después de esto, los dispositivos comienzan a migrar a Kaspersky Security Center Cloud Console.

6. Haga clic en **Finalizar** para cerrar la ventana del Asistente de migración.

7. Si desea buscar y descargar el paquete de instalación independiente nuevamente, vaya a **Detección y despliegue** → **Despliegue y asignación** → **Paquetes de instalación** y haga clic en el botón **Ver la lista de paquetes independientes**. En la lista que se abre, seleccione el paquete de instalación independiente que creó y haga clic en el botón **Descargar**.

Si utiliza Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console en diferentes dispositivos, debe copiar el paquete de instalación independiente en una unidad extraíble o elegir otras formas para transferir el archivo.

Paso 3. Reinstalación del Agente de red en dispositivos administrados a través de Kaspersky Security Center Cloud Console

Después de crear el paquete de instalación independiente del Agente de red, puede crear una tarea de instalación remota. Realizar esta tarea le permite volver a instalar el Agente de red en todos los dispositivos administrados para que estos dispositivos pasen a ser administrados por Kaspersky Security Center Cloud Console.

Para reducir el riesgo de perder datos, le recomendamos que, primero, realice las acciones para un pequeño grupo de administración de hasta 20 dispositivos administrados que se encuentren dentro de la red corporativa y que no incluya servidores físicos. Después de finalizar estas acciones, verifique si la reinstalación se completó con éxito y continúe con su alcance completo.

Para crear una tarea de instalación remota y volver instalar el Agente de red, siga estos pasos:

1. Vuelva al Asistente de migración en Kaspersky Security Center Web Console que se ejecuta de forma local.

   Recomendamos utilizar el Asistente de migración para crear una tarea de instalación remota que reinstale el Agente de red como se describe a continuación. Si es necesario utilizar una tarea de instalación remota personalizada, primero debe crear manualmente un paquete de instalación personalizado desde el paquete de instalación independiente del Agente de red. Tenga en cuenta que al crear un paquete de instalación personalizado, debe especificar la clave "-s" en la línea de comando del archivo ejecutable. De lo contrario, la reinstalación del Agente de red desde este paquete de instalación personalizado se completará con un error.

   Según el estado actual del Asistente de migración, puede realizar una de las siguientes acciones:

   - Si no ha cerrado el Asistente de migración después de la exportación y no ha caducado su sesión, haga clic en el botón **Ir al Paso 3 del Asistente de migración**. Seleccione la casilla de verificación **Cargar paquete de instalación independiente** y haga clic en el botón **Seleccionar paquete de instalación independiente**. En la ventana del navegador que se abre, especifique el paquete de instalación independiente del Agente de red.

   - Si tiene que iniciar el Asistente de migración nuevamente por cualquier motivo, seleccione la casilla de verificación **Cargar paquete de instalación independiente** y haga clic en el botón **Seleccionar paquete de instalación independiente**. En la ventana del navegador que se abre, especifique el paquete de instalación independiente del Agente de red. Después, el Asistente de migración vuelve a mostrar la jerarquía de los grupos de administración de este Servidor de administración. Seleccione el mismo grupo para el que creó el archivo de exportación y haga clic en **Siguiente**.

     El Asistente de migración vuelve a verificar el número total de dispositivos administrados que se incluyen en el grupo de administración seleccionado. Si este número supera los 10 000, aparece un mensaje de error. El botón **Siguiente** permanece no disponible (atenuado) hasta que el número de dispositivos administrados en el grupo de administración seleccionado cae dentro del límite.

2. Espere a que se cargue el paquete de instalación independiente y haga clic en **Siguiente**. El Asistente de migración crea un paquete de instalación personalizada y una tarea de instalación remota para el paquete. La cobertura de la tarea incluirá el grupo de administración que seleccionó en la página **Dispositivos administrados para exportar**. La programación de inicio de la tarea se establecerá en **Manualmente** de forma predeterminada. El Asistente de migración muestra el progreso de la creación. Espere a que los iconos de actualización (🔄) se reemplacen con las marcas de verificación color verde (✓) y haga clic **Siguiente**.

3. Si es necesario, seleccione la casilla de verificación **Ejecutar la tarea de instalación remota recién creada** (desactivada de forma predeterminada) para los dispositivos en el grupo de administración seleccionado del Servidor de administración con ejecución de forma local y todos sus subgrupos. En este caso, los dispositivos se cambiarán a la administración de Kaspersky Security Center Cloud Console, pero solo después de que se complete la instalación del Agente de red. La ruta completa se mostrará al grupo de administración donde se ejecutará la tarea.

La tarea debe iniciarse solo después de que finalice la importación a Kaspersky Security Center Cloud Console. De lo contrario, es posible que los nombres de los dispositivos estén duplicados en la lista.

4. Haga clic en **Finalizar** para cerrar el Asistente de migración e iniciar la tarea de instalación remota para los siguientes propósitos:

   - Actualización de las instancias del Agente de red
   - Cambiar las instancias del Agente de red bajo administración mediante Kaspersky Security Center Cloud Console

   Si ha dejado desmarcada la casilla de verificación **Ejecutar la tarea de instalación remota recién creada**, puede iniciar la tarea más tarde de forma manual, de ser necesario.

Puede comprobar que ahora puede administrar las instancias del Agente de red migradas a través de Kaspersky Security Center Cloud Console. Para ello, vaya a **Activos (dispositivos)** → **Dispositivos administrados**. Asegúrese de que los dispositivos administrados migrados tengan el icono de confirmación (⊘) en las columnas **Visible**, **Agente de red está instalado** y **Agente de red está en ejecución**. Además, asegúrese de que estos dispositivos no tengan la descripción de estado *No conectado durante mucho tiempo*.

Migración con una jerarquía de Servidores de administración

En esta sección se describe la migración de los dispositivos administrados y los objetos relacionados de Kaspersky Security Center Web Console con ejecución de forma local a Kaspersky Security Center Cloud Console. El proceso implica una jerarquía: Kaspersky Security Center Web Console con ejecución de forma local actúa como Servidor de administración secundario y Kaspersky Security Center Cloud Console actúa como Servidor de administración principal.

Cada grupo de administración que transfiera a Kaspersky Security Center Cloud Console debe contener los dispositivos administrados de un solo sistema operativo. Si su red incluye los dispositivos de diferentes sistemas operativos, asígnelos a diferentes grupos de administración y migre cada grupo por separado.

Después de finalizar la migración, todos los Agentes de red del grupo dentro de la cobertura de la migración se actualizan y administran a través de Kaspersky Security Center Cloud Console.

Antes de comenzar, haga lo siguiente:

- Actualización del Servidor de administración que se ejecuta en las instalaciones, hasta la versión 14.2 o posteriores.
- Instale Kaspersky Security Center Web Console versión 12.1 o posterior.
- Actualice el Agente de red en los dispositivos administrados a la versión 12 o posterior.
- En dispositivos Windows, utilice el Agente de red sin una contraseña de desinstalación.

  Si ya se ha establecido la contraseña, realice una de las siguientes acciones en Kaspersky Security Center Web Console:

  - Desactive la opción **Utilizar contraseña de desinstalación** en la Network Agent policy settings.

- Desinstale el Agente de red de forma remota mediante la tarea *Desinstalar aplicación en remoto*. En el campo **Aplicación que se va a desinstalar** de la tarea, seleccione **Agente de red de Kaspersky Security Center**. No olvide introducir la contraseña de desinstalación.

- Actualice las aplicaciones administradas a versiones compatibles con Kaspersky Security Center Cloud Console.

- Asegúrese de tener directivas para las últimas versiones de las aplicaciones administradas. Si sus directivas están desactualizadas, cree directivas nuevas para las versiones compatibles con Kaspersky Security Center Cloud Console.

- Para utilizar directivas reales, actualice los complementos web para las aplicaciones que desea administrar a través de Kaspersky Security Center Cloud Console.

- Desinstalar Aplicaciones Kaspersky desde dispositivos administrados si estas aplicaciones no son compatibles con Kaspersky Security Center Cloud Console.

- Descifre todos los datos (a nivel de disco o de archivo) que Kaspersky Endpoint Security para Windows cifró en los dispositivos administrados que ejecutan el sistema operativo Windows y desactive la función de cifrado en los dispositivos administrados a través de la directiva de la aplicación o de forma local. Para obtener más información, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

  Si el dispositivo Windows aún almacena archivos o carpetas cifrados a través de Kaspersky Endpoint Security para Windows, la actualización del Agente de red se cancelará durante el proceso de migración. Una notificación le pedirá que descifre todos los datos en el dispositivo y que desactive la función de cifrado.

Kaspersky Security Center Cloud Console permite que un Servidor de administración administre un máximo de 25 000 dispositivos administrados.

Para realizar una migración a Kaspersky Security Center Cloud Console, siga los siguientes pasos:

1. Estime la cobertura del proceso de migración, es decir, revise el grupo de administración a exportar, y evalúe la cantidad de dispositivos administrados en él. Asegúrese de que todas las actividades enumeradas como requisitos previos de migración se hayan completado correctamente.

2. En Kaspersky Security Center Cloud Console, vaya al Servidor de administración secundario para los dispositivos administrados que desea migrar.

3. En el menú principal, vaya a **Operaciones** → **Migración**.

   Se abre la página de bienvenida del Asistente de migración.

4. En la página de bienvenida, haga clic en **Siguiente**.

   Se abre la página **Dispositivos administrados para exportar** que muestra toda la jerarquía de grupos de administración del Servidor de administración secundario.

5. En la página **Dispositivos administrados para exportar**, haga clic en el icono de flecha (>) junto al lado del nombre de grupo **Dispositivos administrados** y, después, expanda la jerarquía de los grupos de administración. Seleccione el grupo de administración que desea exportar.

El Asistente de migración verifica el número total de dispositivos administrados que se incluyen en el grupo de administración seleccionado. Si este número supera los 10 000, aparece un mensaje de error. El botón **Siguiente** permanece no disponible (atenuado) hasta que el número de dispositivos administrados en el grupo de administración seleccionado cae dentro del límite.

6. Seleccione las aplicaciones administradas cuyas directivas y tareas deben transferirse a Kaspersky Security Center Cloud Console junto con los objetos de grupo. Para seleccionar las aplicaciones administradas cuyos objetos se exportarán, seleccione las casillas de verificación junto a sus nombres en la lista.

   A pesar de que el Servidor de administración de Kaspersky Security Center se encuentra en la lista, al seleccionar la casilla de verificación correspondiente no se exportan sus directivas.

   Para asegurarse de que las aplicaciones administradas sean compatibles con Kaspersky Security Center Cloud Console, haga clic en el enlace correspondiente. Este le redirigirá al tema de Ayuda en línea que contiene la lista de aplicaciones administradas por Kaspersky Security Center Cloud Console.

   Si selecciona aplicaciones que no sean compatibles con Kaspersky Security Center Cloud Console, las directivas y las tareas de estas aplicaciones se migrarán de todos modos. No obstante, no podrá administrarlas en Kaspersky Security Center Cloud Console debido a la falta de disponibilidad de complementos dedicados.

7. Ver la lista de objetos de grupo exportados de forma predeterminada. También puede especificar objetos que no sean de grupo para que se exporten junto con el grupo de administración seleccionado, si fuera necesario, como tareas globales, selecciones de dispositivos personalizados, informes, funciones personalizadas, usuarios internos y grupos de seguridad, y categorías de aplicaciones personalizadas con contenido añadido manualmente. Esta página incluye las siguientes secciones:

   - **Tareas globales**

     La lista de tareas globales de las aplicaciones administradas, así como las tareas globales del Agente de red.

     Si una tarea global seleccionada se aplica a una selección de objeto específica, esta selección también se exportará.

     Aunque las tareas globales del Servidor de administración se encuentran en la lista, no puede exportarlas. Seleccionar dichas tareas no afecta el alcance de la exportación. Las tareas de instalación remota también quedan fuera del alcance de la exportación, porque sus respectivos paquetes de instalación no se pueden exportar.

   - **Selecciones de dispositivos**

     La lista de selecciones de dispositivos personalizadas.

   - **Informes**

La lista editable de instancias de informes que se exportarán.

Si un informe seleccionado se aplica a una selección de objeto específica, esta selección también se exportará.

Kaspersky Security Center Cloud Console tiene el mismo conjunto de plantillas de informes que Kaspersky Security Center Web Console, por lo que puede seleccionar para exportar solo los informes que creó manualmente o volvió a configurar.

- **Objetos de grupo**

La lista de objetos de grupo que se exportarán de forma predeterminada. Los siguientes objetos relacionados con el grupo de administración seleccionado se exportarán de forma predeterminada en su totalidad:

- La estructura del grupo de administración, es decir, todos los subgrupos del grupo de administración seleccionado
- Los dispositivos incluidos en los grupos de administración que se exportarán
- Las etiquetas asignadas a los dispositivos que se exportarán.

  Si se creó una etiqueta en Kaspersky Security Center Web Console, pero nunca se la asignó a ningún dispositivo, entonces no se exportará. Las reglas del etiquetado automático tampoco se exportarán.

- Las directivas de grupo de las aplicaciones administradas que se han seleccionado

  Las directivas del Servidor de administración y las directivas del Agente de red no se exportan.

- Tareas de grupo de las aplicaciones administradas que han sido seleccionadas y tareas de grupo del Agente de Red.

  Las tareas del Servidor de administración no se exportan.

También puede evitar que se exporten determinados tipos de objetos que no sean de grupo:

- Para cancelar la exportación de funciones personalizadas (es decir, aquellas creadas solo por el usuario), seleccione la casilla de verificación **Excluir funciones personalizadas de la exportación**.
- Para cancelar la exportación de usuarios internos y grupos de seguridad, seleccione la casilla de verificación **Excluir usuarios internos y grupos de seguridad de la exportación**.
- Para cancelar la exportación de categorías de aplicaciones personalizadas con contenido añadido manualmente, seleccione la casilla de verificación **Excluir categorías de aplicaciones personalizadas de la exportación**.

Si transfiere dispositivos de varios sistemas operativos a Kaspersky Security Center Cloud Console, los objetos que no sean de grupo solo se deben migrar una vez.

8. Después de definir la cobertura de la migración, haga clic en **Siguiente** para comenzar el proceso de exportación. Se abre la página **Creando el archivo de exportación**, donde puede ver el progreso de la exportación para cada tipo de objeto que incluyó en la cobertura de la migración. Espere a que cada uno de los iconos de actualización (🔄) ubicados junto a cada elemento de la lista de objetos se reemplacen con marcas de verificación color verde (✓). Cuando la exportación finaliza, el archivo de exportación se guarda automáticamente en una carpeta temporal. Se abre la siguiente página que muestra la jerarquía completa de los grupos de administración en Kaspersky Security Center Cloud Console, que actúa como el Servidor de administración principal.

9. Seleccione la casilla de verificación junto al grupo de administración en el que se deben importar los objetos de grupo y, luego, haga clic en **Siguiente**. El archivo se desempaqueta; y los objetos de grupo y los que no son de grupo se restauran al grupo de administración de destino.

   Si el nombre del objeto que desea restaurar es idéntico al nombre de un objeto existente, al primero se le añade un sufijo progresivo.

   Cuando termina la importación, la estructura exportada de los grupos de administración, incluidos los detalles de los dispositivos, aparece debajo del grupo de administración de destino que ha seleccionado. También se importan los objetos que no son de grupo.

   No podrá minimizar el Asistente de migración ni realizar ninguna operación simultánea durante la importación. Espere a que cada uno de los iconos de actualización (🔄) ubicados junto a cada elemento de la lista de objetos se reemplacen con marcas de verificación color verde (✓) y finalice la importación. Después de esto, los dispositivos comienzan a migrar a Kaspersky Security Center Cloud Console.

10. Una vez completada la importación, el Asistente de migración muestra una lista de los paquetes de instalación del Agente de red disponibles en Kaspersky Security Center Cloud Console para un sistema operativo adecuado. Seleccione el paquete de instalación que contenga la versión relevante y la localización del Agente de red.

    Seleccione el paquete de instalación del Agente de red para Windows de Kaspersky solo si completó previamente el asistente de inicio rápido en el espacio de trabajo de Kaspersky Security Center Cloud Console y si realiza la migración de dispositivos Windows.

11. Haga clic en **Siguiente**.

    El Asistente de migración crea un nuevo paquete de instalación independiente (o utiliza uno existente) y un paquete de instalación personalizada basado en este, así como la tarea de instalación remota correspondiente. La cobertura de la tarea incluye el grupo de administración seleccionado en la página **Dispositivos administrados para exportar**. La programación de inicio de la tarea se establece en **Manualmente** de manera predeterminada. El Asistente de migración muestra el progreso de la creación.

12. Espere a que todos los iconos de actualización (🔄) se reemplacen con las marcas de verificación color verde (✓) y, luego, haga clic en **Siguiente**.

13. Si es necesario, seleccione la casilla de verificación **Ejecutar la tarea de instalación remota recién creada** (desactivada de forma predeterminada) para los dispositivos en el grupo de administración seleccionado en Kaspersky Security Center Web Console con ejecución de forma local y todos sus subgrupos. Una vez completada la instalación del Agente de red, puede administrar los dispositivos seleccionados a través de Kaspersky Security Center Cloud Console. La ruta completa se muestra al grupo de administración donde se ejecutará la tarea.

La tarea de instalación remota debe iniciarse solo después de que finalice la importación a Kaspersky Security Center Cloud Console. De lo contrario, los dispositivos pueden duplicarse.

14. Haga clic en **Finalizar** para cerrar el Asistente de migración e iniciar la tarea de instalación remota para los siguientes propósitos:

    - Actualización de las instancias del Agente de red
    - Administrar las instancias del Agente de red a través de Kaspersky Security Center Cloud Console

    Si ha dejado desactivada la casilla de verificación **Ejecutar la tarea de instalación remota**, podrá iniciar la tarea manualmente más tarde, de ser necesario.

Puede comprobar que ahora puede administrar las instancias del Agente de red migradas a través de Kaspersky Security Center Cloud Console. Para ello, vaya a **Activos (dispositivos)** → **Dispositivos administrados**. Asegúrese de que los dispositivos administrados migrados tengan el icono de confirmación (✓) en las columnas **Visible**, **Agente de red está instalado** y **Agente de red está en ejecución**. Además, asegúrese de que estos dispositivos no tengan la descripción de estado *No conectado durante mucho tiempo*.

Escenario: migración de dispositivos con sistemas operativos Linux o macOS

Esta sección describe cómo migrar los dispositivos que ejecutan sistemas operativos Linux o macOS desde Kaspersky Security Center Web Console que se ejecuta de forma local a Kaspersky Security Center Cloud Console. Los escenarios básicos de migración sin una jerarquía de Servidores de administración y migración con dicha jerarquía permiten transferir todos los dispositivos y objetos relacionados a Kaspersky Security Center Cloud Console. Sin embargo, si su red incluye dispositivos que ejecutan no solo Windows, sino también Linux o macOS, debe transferir los dispositivos de cada tipo de sistema operativo por separado. Como consecuencia, debe realizar la migración varias veces.

Requisitos previos

Antes de comenzar, haga lo siguiente:

- Actualice el Servidor de administración que se ejecuta de forma local hasta la versión 12 Revisión A o versiones posteriores.
- Instale Kaspersky Security Center Web Console versión 12.1 o posterior.
- Actualice el Agente de red en los dispositivos administrados a la versión 12 o posterior.
- Actualice las aplicaciones administradas a versiones compatibles con Kaspersky Security Center Cloud Console.
- Asegúrese de tener directivas para las últimas versiones de las aplicaciones administradas. Si sus directivas están desactualizadas, cree directivas nuevas para las versiones compatibles con Kaspersky Security Center Cloud Console.

- Para utilizar directivas reales, actualice los complementos web para las aplicaciones que desea administrar a través de Kaspersky Security Center Cloud Console.
- Desinstale las aplicaciones de Kaspersky de los dispositivos administrados si estas aplicaciones no son compatibles con Kaspersky Security Center Cloud Console. Después, reemplace las aplicaciones desinstaladas por otras compatibles.

Kaspersky Security Center Cloud Console permite que un Servidor de administración administre un máximo de 25 000 dispositivos administrados.

Etapas de la migración

La migración a Kaspersky Security Center Cloud Console comprende las siguientes etapas:

1. **Agrupar dispositivos administrados por sus sistemas operativos**

   Si su red tiene dispositivos con sistemas operativos diferentes (Windows, Linux o macOS), coloque los dispositivos con cada sistema operativo en grupos de administración separados dentro de Kaspersky Security Center Web Console. Además, cree un grupo de administración para cada distribución de Linux. Por ejemplo, si tiene dispositivos Debian y Red Hat Linux, asígnelos a diferentes grupos de administración. Esto le permitirá realizar la migración correctamente dado que se requieren diferentes paquetes de instalación del Agente de red para varios sistemas operativos.

2. **Realizar por separado la migración de cada grupo de administración y los objetos de la aplicación**

   Los dispositivos administrados de cada sistema operativo deben migrarse por separado, para incluir sus directivas y tareas. Por ejemplo, si tiene dispositivos Windows, macOS, Ubuntu y CentOS, primero transfiera los dispositivos que ejecutan el sistema operativo Windows a Kaspersky Security Center Cloud Console, después, macOS, Ubuntu y, finalmente, CentOS. Puede transferir los dispositivos administrados en cualquier orden.

   Para hacer esto, realice la migración sin la jerarquía de Servidores de administración o la migración con dicha jerarquía, dependiendo de si su red incluye Servidores de administración secundarios. Durante la migración, utilice el paquete de instalación del Agente de red correspondiente al sistema operativo de los dispositivos transferidos. Por ejemplo, seleccione el Agente de red de Kaspersky Security Center 13.2 para dispositivos Linux a fin de realizar la migración correctamente.

   Tenga en cuenta que los objetos que no son de grupo, como tareas globales, selecciones de dispositivos personalizados o informes, solo deben migrarse una vez.

Resultados

Al finalizar la migración, puede asegurarse de que se haya realizado correctamente:

- La versión adecuada de Agente de red se ha reinstalado en cada dispositivo administrado que ejecuta el sistema operativo Linux o macOS.
- Todos los dispositivos Linux o macOS se administran a través de Kaspersky Security Center Cloud Console.
- Se conservan todas las configuraciones de objetos que se utilizaban antes de la migración.

Escenario: Migración inversa de Kaspersky Security Center Cloud Console a Kaspersky Security Center

Es posible que desee migrar los dispositivos administrados de Kaspersky Security Center Cloud Console a Servidor de administración de Kaspersky Security Center. Este proceso se puede utilizar, por ejemplo, para revertir la migración a Kaspersky Security Center Cloud Console.

Requisitos previos

Antes de comenzar, asegúrese de que se cumplan los siguientes requisitos previos:

- Kaspersky Security Center Cloud Console está disponible y tiene dispositivos administrados conectados.
- El Servidor de administración de Kaspersky Security Center 14.2 (o versión posterior) está disponible y tiene un paquete de instalación para la versión 13 (o posterior) del Agente de red.

Etapas de migración inversa

La migración inversa comprende las siguientes etapas:

1. **Crear un paquete de instalación independiente de Agente de red en la instancia local del Servidor de administración de Kaspersky Security Center**

   En el servidor de administración de Kaspersky Security Center que se ejecuta localmente, cree un paquete de instalación independiente de Agente de red.

   Durante el proceso de creación, puede seleccionar la opción **Mover dispositivos no asignados a este grupo** para especificar el grupo de administración al que desea mover Agentes de red después de la instalación. Si ha especificado el grupo de administración, se crea una regla de traslado automático que moverá al grupo de administración objetivo a todos los Agentes de red instalados con este paquete de instalación independiente.

   > Para garantizar una migración inversa correcta, asegúrese de seleccionar una versión del Agente de red que sea igual o posterior a la versión utilizada en Kaspersky Security Center Cloud Console.

2. **Creación de un paquete de instalación personalizada en Kaspersky Security Center Cloud Console**

   En Kaspersky Security Center Cloud Console, cree un paquete de instalación personalizado basado en el paquete de instalación independiente que creó y guardó desde el Servidor de administración de Kaspersky Security Center que se ejecuta en los predios del cliente.

   Para activar la instalación del paquete en modo silencioso, en el campo **Línea de comando del archivo ejecutable**, especifique la clave `-s`.

3. **Creación de una tarea de instalación remota**

   En Kaspersky Security Center Cloud Console, cree una tarea de instalación remota utilizando el paquete de instalación personalizada que ha creado.

4. **Ejecución de la tarea de instalación remota**

   Inicie la tarea de instalación remota que ha creado. La tarea inicia la reinstalación de todos los Agentes de red en el grupo de administración especificado y también cambia los Agentes de red bajo la administración del Servidor de administración de Kaspersky Security Center que se ejecuta localmente, por medio del cambio de la dirección de conexión y la modificación de otros ajustes de conexión.

Si no especificó ningún grupo de administración de destino durante la creación del paquete de instalación independiente, todos los dispositivos se moverán al grupo **Dispositivos no asignados**.

Resultados

Al finalizar la migración, puede asegurarse de que se haya realizado correctamente:

- Todos los dispositivos dentro de la cobertura de la tarea de instalación remota que antes se administraban mediante Kaspersky Security Center Cloud Console pasan a administrarse mediante el Servidor de administración de Kaspersky Security Center que se ejecuta en los predios del cliente.
- Los dispositivos se mueven automáticamente al grupo de administración especificado en la configuración del paquete de instalación.

La tarea de instalación remota en Kaspersky Security Center Cloud Console no se puede completar: no tiene más dispositivos de destino ya que todos tienen sus configuraciones de conexión modificadas. Debe detener la tarea manualmente después de asegurarse de que el icono de error ( ) ha aparecido en la columna **Visible** de la lista Dispositivos administrados para todos los dispositivos de la cobertura de la migración.

Migración con Servidores de administración virtuales

Si tiene servidores de administración virtuales en su infraestructura local existente de Kaspersky Security Center, no puede migrar de Kaspersky Security Center local a Kaspersky Security Center Cloud Console usando el Asistente de migración. Además, solo podrá migrar los dispositivos de sus clientes. Deberá crear directivas, tareas e informes manualmente.

Puede seguir uno de los siguientes escenarios de migración:

- Trasladar los dispositivos de su cliente de los Servidores de administración virtuales a un Servidor de administración principal.
- Realizar la migración manual desde servidores de administración virtuales.

Escenario: migración con servidores de administración virtuales mediante el traslado de dispositivos

Para realizar la migración de Kaspersky Security Center Web Console que se ejecuta en las instalaciones a Kaspersky Security Center Cloud Console, puede mover sus dispositivos de los Servidores de administración virtuales a un Servidor de administración principal.

Requisitos previos

Antes de la migración, debe realizar una serie de acciones, entre ellas la actualización del Servidor de administración que se ejecuta localmente a la versión 12 o posteriores y la actualización de las aplicaciones administradas a las versiones compatibles con Kaspersky Security Center Cloud Console.

Escenario de migración

El escenario avanza en etapas:

1. **Creación de un grupo de administración para cada uno de sus Servidores de administración virtuales**

   El grupo se crea en la instancia de Kaspersky Security Center que se ejecuta localmente.

2. **Traslade los dispositivos de sus clientes**

   En la instancia local de Kaspersky Security Center, traslade los dispositivos de sus clientes de cada Servidor de administración virtual al grupo de administración respectivo creado en la etapa anterior.

3. **Migración**

   Realice la migración como se describe para la red sin una jerarquía de servidores de administración.

4. **Mover dispositivos bajo la administración de los Servidores de administración virtual (paso opcional)**

   Si desea administrar a sus clientes a través de los Servidores de administración virtual, mueva los dispositivos de los grupos de administración bajo la administración de los Servidores de administración virtual.

5. **Cree directivas, tareas e informes**

   Cree directivas, tareas e informes según sea necesario.

Resultados

Al finalizar la migración, puede asegurarse de que se haya realizado correctamente:

- El Agente de red se reinstaló en todos los dispositivos administrados.
- Todos los dispositivos se administran a través de Kaspersky Security Center Cloud Console.
- Se conservan todas las configuraciones de objetos que se utilizaban antes de la migración.

Escenario: migración manual con servidores de administración virtuales

Puede migrar de Kaspersky Security Center Web Console que se ejecuta localmente a Kaspersky Security Center Cloud Console manualmente.

Requisitos previos

Antes de la migración, debe realizar una serie de acciones, entre ellas la actualización del Servidor de administración que se ejecuta localmente a la versión 12 o posteriores y la actualización de las aplicaciones administradas a las versiones compatibles con Kaspersky Security Center Cloud Console.

Escenario de migración

El escenario avanza en etapas:

1. **Creación de un grupo de administración para cada uno de sus Servidores de administración virtuales**

En Kaspersky Security Center Cloud Console, cree un grupo de administración que corresponda a cada uno de sus Servidores de administración virtuales.

2. **Creación de un paquete de instalación independiente para el Agente de red**

   Cree un paquete de instalación independiente para el Agente de red. Durante la creación, especifique el grupo de administración que ha creado en la etapa anterior. Esto significa que debe crear un paquete de instalación independiente para cada grupo de administración.

   Esta etapa ocurre en su Kaspersky Security Center Cloud Console.

3. **Descarga de paquetes de instalación independientes**

   Descargue los paquetes de instalación independientes que ha creado en la etapa anterior. Esta etapa ocurre en su Kaspersky Security Center Cloud Console.

4. **Crear un archivo con cada paquete de instalación independiente**

   Los tipos de archivos comprimidos disponibles son: ZIP, CAB, TAR o TAR.GZ.

5. **Creación de paquetes de instalación personalizada para el Agente de red**

   Cree paquetes de instalación personalizada para el Agente de red. Durante la creación, use los archivos que ha creado en la etapa anterior.

   Esta etapa se realiza en la instancia de Kaspersky Security Center que se ejecuta localmente.

6. **Creación de tareas de instalación remota**

   Cree tareas de instalación remota para instalar Agente de red a partir de los paquetes de instalación personalizada creados.

   Al crear una tarea, especifique el grupo de administración correspondiente.

   Esta etapa se realiza en la instancia de Kaspersky Security Center que se ejecuta localmente.

7. **Ejecutar las tareas de instalación remota creadas**

   Los agentes de red se actualizan. El servidor de administración de Kaspersky Security Center Cloud Console se hace cargo de la administración de los mismos.

   Todos los dispositivos migran a Kaspersky Security Center Cloud Console y se colocan en los grupos de administración que se especificaron cuando creó los paquetes de instalación independientes para Agente de red.

8. **Mover dispositivos bajo la administración de los Servidores de administración virtual (paso opcional)**

   Si desea administrar a sus clientes a través de los Servidores de administración virtual, mueva los dispositivos de los grupos de administración bajo la administración de los Servidores de administración virtual.

9. **Cree directivas, tareas e informes**

   Cree directivas, tareas e informes según sea necesario.

Resultados

Al finalizar la migración, puede asegurarse de que se haya realizado correctamente:

- El Agente de red se reinstaló en todos los dispositivos administrados.
- Todos los dispositivos se administran a través de Kaspersky Security Center Cloud Console.

  Se conservan todas las configuraciones de objetos que se utilizaban antes de la migración.

Escenario: mover dispositivos desde los grupos de administración bajo la administración de servidores virtuales

Es posible que desee administrar a sus clientes a través de los Servidores de administración virtual. Si migró dispositivos y otros elementos de Kaspersky Security Center en las instalaciones a Kaspersky Security Center Cloud Console, los dispositivos se encuentran en los grupos de administración. Para administrar los dispositivos de los clientes a través de Servidores de administración virtual, debe mover los dispositivos de los grupos de administración bajo la administración de Servidores de administración virtual.

Requisitos previos

Ha creado un Servidor de administración virtual para cada uno de sus clientes.

Todos los dispositivos de cada cliente se encuentran en un grupo de administración individual.

Etapas

El escenario avanza en etapas:

1. **Creación de un paquete de instalación independiente para el Agente de red**

   Cambie a cada uno de los Servidores de administración virtual creados y, luego, cree un paquete de instalación independiente del Agente de red. Para cambiar los Servidores de administración en el menú principal, haga clic en el icono de flecha (▶) a la derecha del nombre del Servidor de administración actual y, luego, seleccione el Servidor de administración requerido.

2. **Descarga de paquetes de instalación independientes**

   Descargue los paquetes de instalación independientes que ha creado en la etapa anterior.

3. **Cree un archivo con cada paquete de instalación independiente**

   Los tipos de archivos comprimidos disponibles son: ZIP, CAB, TAR o TAR.GZ.

4. **Creación de paquetes de instalación personalizada para el Agente de red**

   Cree paquetes de instalación personalizada para el Agente de red. Durante la creación, use los archivos que ha creado en la etapa anterior.

   Esta etapa ocurre en el Servidor de administración principal.

5. **Creación de tareas de instalación remota**

   Cree tareas de instalación remota para instalar Agente de red a partir de los paquetes de instalación personalizada creados.

   Al crear una tarea, especifique el grupo de administración correspondiente.

   Esta etapa ocurre en el Servidor de administración principal.

6. **Ejecute las tareas de instalación remota creadas**

   Los agentes de red se actualizan. Los dispositivos se mueven bajo la administración de los Servidores de administración virtual.

7. **Cree directivas, tareas e informes**

Cree directivas, tareas e informes según sea necesario.

Resultados

Ahora puede administrar los dispositivos de los clientes migrados mediante servidores de administración virtuales.

Acerca de la migración de Pro View a Expert View:

La migración solo está disponible si tiene una licencia de Kaspersky Next.

Para acceder a una descripción detallada del procedimiento de migración, consulte la Ayuda de Kaspersky Endpoint Security Cloud.

Una vez finalizada la migración, se creará un nuevo espacio de trabajo enExpert View y recibirá la notificación por correo electrónico correspondiente. El nuevo espacio de trabajo tiene el mismo nombre que el espacio de trabajo en Pro View.

Vaya al nuevo espacio de trabajo y asegúrese de que los objetos se transfieran de la siguiente manera:

- La licencia de Kaspersky Next se muestra en la sección **Licencias** y en la ventana de propiedades del Servidor de administración.
- En el menú principal, vaya a **Activos (dispositivos)**→ **Dispositivos administrados**.

  Todos los dispositivos que ejecutan Windows y macOS aparecerán en la lista de dispositivos administrados.

  Los dispositivos transferidos se conectan automáticamente al espacio de trabajo creado en Expert View. Esto puede demorar un poco.
- En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.

  En la lista de directivas, aparecerá la directiva del Agente de red con la protección con contraseña configurada.

Asistente de inicio rápido

Esta sección brinda información sobre el asistente de inicio rápido de Kaspersky Security Center Cloud Console.

Acerca del asistente de inicio rápido

El asistente de inicio rápido en Kaspersky Security Center Cloud Console le permite crear un mínimo de tareas y directivas necesarias, ajustar un mínimo de valores y comenzar a crear paquetes de instalación de las aplicaciones de Kaspersky. Con el asistente, puede realizar los cambios siguientes en Kaspersky Security Center Cloud Console:

- Iniciar la descarga de paquetes de instalación para las aplicaciones administradas de Kaspersky.
- Crear un paquete de instalación independiente de Agente de red para los dispositivos que ejecutan Windows, Linux o macOS.
- Crear una directiva del Agente de red de Kaspersky Security Center.
- Cree la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*.
- Crear directivas y tareas para las aplicaciones administradas de Kaspersky.
- Configurar la interacción con Kaspersky Security Network (KSN).

Una vez finalizado el asistente de inicio rápido, los paquetes de instalación del Agente de red y las aplicaciones administradas de Kaspersky aparecen en la lista **Detección y despliegue → Despliegue y asignación → Paquetes de instalación**.

El asistente de inicio rápido crea directivas para las aplicaciones administradas, como Kaspersky Endpoint Security para Windows, a menos que dichas directivas ya se creen para el grupo de dispositivos administrados. El asistente de inicio rápido crea tareas si no existen tareas con los mismos nombres para el grupo de dispositivos administrados.

Kaspersky Security Center Cloud Console solicita automáticamente ejecutar el asistente de inicio rápido después de haber creado un espacio de trabajo de la empresa y de haber iniciado por primera vez Kaspersky Security Center Cloud Console. También puede iniciar el asistente de inicio rápido manualmente en cualquier momento.

Inicio del asistente de inicio rápido

Kaspersky Security Center Cloud Console solicita automáticamente ejecutar el asistente de inicio rápido después de haber creado un espacio de trabajo de la empresa y de haber iniciado por primera vez Kaspersky Security Center Cloud Console. También puede iniciar el asistente de inicio rápido manualmente en cualquier momento.

Si vuelve a iniciar el asistente de inicio rápido, las tareas y directivas creadas en la ejecución anterior del asistente no se crean de nuevo.

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**.

   De forma alternativa, puede iniciar el asistente de inicio rápido seleccionando **Detección y despliegue** → **Despliegue y asignación** → **Asistente de inicio rápido**.

El asistente le solicita que realice la configuración inicial de Kaspersky Security Center Cloud Console. Siga las instrucciones del asistente. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente. Utilice el botón **Atrás** para volver al paso anterior del asistente.

Paso 1. Seleccionar paquetes de instalación para descargar

En la lista, seleccione las aplicaciones de Kaspersky que desea instalar en los dispositivos del cliente. Kaspersky Security Center Cloud Console creará paquetes de instalación para las aplicaciones seleccionadas. Luego, usará los paquetes de instalación creados para instalar las aplicaciones.

Al seleccionar un paquete de instalación para descargar, preste atención al idioma: los paquetes de instalación están disponibles en diferentes idiomas.

Seleccione las siguientes aplicaciones:

- Agente de red de Kaspersky Security Center

  Al seleccionar los paquetes de instalación del Agente de red, tenga en cuenta lo siguiente:

  - El Agente de red debe estar instalado en cada dispositivo cliente. Por lo tanto, seleccione un Agente de red apropiado para cada sistema operativo que se ejecute en los dispositivos cliente.

  - El Agente de red debe instalarse manualmente mediante un paquete de instalación independiente en el dispositivo que seleccione para actuar como punto de distribución. Se requieren puntos de distribución para realizar sondeos de red y para la instalación remota de aplicaciones de seguridad de Kaspersky en los dispositivos cliente. Por lo tanto, debe seleccionar al menos un paquete de instalación del Agente de red. Mientras continúa con los siguientes pasos del asistente, Kaspersky Security Center Cloud Console crea el paquete de instalación independiente del Agente de red.

    En comparación con los puntos de distribución basados en Windows, los puntos de distribución basados en Linux y macOS tienen una funcionalidad limitada. Le recomendamos que seleccione equipos con Windows para que actúen como puntos de distribución.

    Puede seleccionar Agentes de red para Windows, Linux y macOS. Si selecciona un Agente de red solo para un sistema operativo, por ejemplo, macOS, se creará un paquete de instalación independiente para el sistema operativo seleccionado. Si selecciona Agente de red para varios sistemas operativos, Kaspersky Security Center Cloud Console crea solo un paquete de instalación independiente de acuerdo con las siguientes prioridades: Windows es la máxima prioridad, y le siguen Linux y luego macOS. Por ejemplo, si selecciona Agentes de red para Linux y macOS, Kaspersky Security Center Cloud Console crea un paquete de instalación independiente para el Agente de red para Linux. Puede crear un paquete de instalación independiente de Agente de red manualmente para cualquiera de estos sistemas operativos en cualquier momento.

- Aplicaciones de seguridad de Kaspersky

  Seleccione los paquetes de instalación apropiados para los sistemas operativos instalados en los dispositivos cliente de su organización.

Paso 2. Configuración de un servidor proxy

Si su organización utiliza un servidor proxy para conectarse a Internet, especifique la configuración del servidor proxy en este paso del asistente. Esta configuración se agrega al paquete de instalación del Agente de red. Después de la instalación, el Agente de red usa automáticamente esta configuración en cada dispositivo cliente.

Especifique la configuración siguiente para la conexión con el servidor proxy:

- **Usar servidor proxy**
- **Dirección**
- **Número de puerto**
- **Autenticación del servidor proxy**

  Si esta opción está activada, podrá especificar las credenciales de autenticación del servidor proxy en los campos de entrada.

  Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.

  Esta opción está deshabilitada de manera predeterminada.

- **Nombre de usuario**

  El nombre de usuario de la cuenta con la que se establece la conexión al servidor proxy.

  Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.

- **Contraseña**

  La contraseña de usuario de la cuenta con la que se establece la conexión al servidor proxy.

  Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.

Paso 3. Configurar Kaspersky Security Network

Si en el primer paso del asistente descargó el paquete de instalación de Kaspersky Endpoint Security para Windows, se muestra el texto de la Declaración de KSN para las siguientes aplicaciones:

- Kaspersky Endpoint Security para Windows
- Kaspersky Security Center instalado en dispositivos locales
- Kaspersky Security Center Cloud Console instalado en el entorno de nube

Si no descargó el paquete de instalación de Kaspersky Endpoint Security para Windows, no se muestra la Declaración de KSN para esta aplicación.

En el modo de prueba, solo se muestra la Declaración de KSN para Kaspersky Endpoint Security para Windows.

Lea atentamente la Declaración de Kaspersky Security Network. Seleccione una de las siguientes opciones:

- **Acepto usar Kaspersky Security Network**

  Kaspersky Security Center Cloud Console 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 Cloud Console y las aplicaciones administradas no proporcionarán información a Kaspersky Security Network.

  Si selecciona esta opción, se deshabilitará el uso de Kaspersky Security Network.

De forma predeterminada, el uso de KSN está desactivado. Más adelante, si cambia de opinión sobre el uso de KSN, puede activar (o desactivar) la opción correspondiente en la ventana de propiedades del Servidor de administración, en la sección **Configuración de KSN**.

Paso 4. Configuración de la administración de actualizaciones de terceros

Este paso no se muestra si la tarea *Buscar vulnerabilidades y actualizaciones requeridas* ya existe.

Si desea obtener una lista de actualizaciones para las aplicaciones instaladas en los dispositivos administrados y una lista de vulnerabilidades encontradas y correcciones recomendadas para ellas, active la opción **Buscar actualizaciones de software y reparaciones de vulnerabilidades de terceros**. Si esta opción está activada, Kaspersky Security Center Cloud Console crea la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

Paso 5. Creación de una configuración básica de protección de la red

En este paso del asistente, haga clic en el botón **Crear** para crear los objetos necesarios para la protección inicial de sus dispositivos cliente.

Kaspersky Security Center Cloud Console realiza dos operaciones:

- Crear directivas y tareas básicas con configuraciones predeterminadas

  Se crean las siguientes directivas:

  - Directiva del Agente de red de Kaspersky Security Center
  - Directivas para aplicaciones de Kaspersky administradas

Se crean las siguientes tareas:

- La tarea *Descargar actualizaciones en los repositorios de puntos de distribución*
- Tarea *Buscar vulnerabilidades y actualizaciones requeridas*

  Esta tarea solo se crea si ha activado la opción **Buscar actualizaciones de software y reparaciones de vulnerabilidades de terceros** en el paso anterior del asistente.
- Tareas para aplicaciones de Kaspersky administradas

- Creación de un paquete de instalación independiente para el Agente de red

  Utilizará este paquete para instalar Agente de red en los puntos de distribución. Kaspersky Security Center Cloud Console crea el paquete de instalación independiente basándose en el paquete de instalación de Agente de red que seleccionó en el paso anterior del asistente. Durante la creación del paquete, debe leer y aceptar los términos de EULA para Agente de red. Una vez creado el paquete de instalación independiente, se le solicitará que lo descargue al dispositivo que está utilizando en este momento.

  La creación del paquete de instalación independiente del Agente de red puede llevar unos momentos. Puede continuar con el siguiente paso del asistente. El proceso continuará en modo de segundo plano. Si es necesario, puede realizar un seguimiento del estado de descarga del paquete de instalación en la columna **Estado del paquete** (**Detección y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**).

  Para fines de autenticación, cada paquete de instalación independiente se firma con un certificado. El certificado se vuelve a emitir de vez en cuando. Después de cada procedimiento de reemisión del certificado, Kaspersky Security Center Cloud Console actualiza automáticamente las firmas de todos los paquetes de instalación independientes creados. Para los paquetes de instalación independientes descargados, no se puede realizar la actualización automática de firma. Por lo tanto, el certificado caduca y puede producirse un error de certificado cuando instale una aplicación desde un paquete de instalación independiente. En este caso, vuelva a descargar el paquete de instalación independiente.

Paso 6. Cerrar el asistente de inicio rápido

En la página de finalización del asistente de inicio rápido, lea sobre las operaciones adicionales que debe realizar para implementar las aplicaciones de seguridad de Kaspersky en los dispositivos cliente. Siga las etapas previstas en el escenario de despliegue inicial de aplicaciones Kaspersky.

Despliegue inicial de las aplicaciones de Kaspersky

Esta sección describe el despliegue inicial de las aplicaciones de Kaspersky en los dispositivos cliente de su organización.

Escenario: despliegue inicial de aplicaciones de Kaspersky

Este escenario describe cómo instalar aplicaciones de Kaspersky en dispositivos cliente en Kaspersky Security Center Cloud Console. Primero, debe implementar puntos de distribución en su red. Luego, por medio de los puntos de distribución, debe realizar un sondeo de red y detectar dispositivos en red en su red. Después de eso, puede instalar aplicaciones de Kaspersky en dispositivos en red.

Cuando se completa el escenario, las aplicaciones de Kaspersky quedan implementadas en los dispositivos cliente seleccionados en la red de su organización. Puede administrar todos los dispositivos con aplicaciones de Kaspersky instaladas.

Requisitos previos

Antes de comenzar, asegúrese de que se cumplan los siguientes requisitos previos:

- El asistente de inicio rápido ha terminado.
- Se han creado los paquetes de instalación del Agente de red y las aplicaciones de seguridad.
- La dirección https://aes.s.kaspersky-labs.com/endpoints/ se incluye en las excepciones de firewall de dispositivos administrados.
- Tiene información sobre la configuración de Internet para los dispositivos cliente de su organización e información sobre la pasarela y la configuración del servidor proxy.
- Los dispositivos cliente de su organización no están cifrados.

Etapas

El despliegue inicial de las aplicaciones de Kaspersky se realiza en etapas:

1. **Seleccionar un dispositivo para que actúe como un punto de distribución**

   En Kaspersky Security Center Cloud Console, un punto de distribución está destinado a:

   - Sondeo de red y detección de dispositivos
   - Instalación remota del Agente de red en dispositivos cliente
   - Conexión de dispositivos cliente al Servidor de administración (cuando un punto de distribución actúa como pasarela de conexión)

   Seleccione un dispositivo en la red de su organización para que actúe como punto de distribución para un grupo de administración. El dispositivo seleccionado debe cumplir con los requisitos para puntos de distribución. Según la cantidad de dispositivos cliente en la red de su organización, seleccione la cantidad correcta de dispositivos que deben actuar como puntos de distribución.

2. **Creación de un paquete de instalación independiente para el Agente de red**

   Cree un paquete de instalación independiente del Agente de red para instalarlo en el punto de distribución.

   Si sus dispositivos cliente no tienen acceso directo a Internet para conectarse al Servidor de administración, en Configuración del paquete de instalación del Agente de red, configure la pasarela de conexión y el servidor proxy.

3. **Instalación del Agente de red en el dispositivo seleccionado para que funcione como un punto de distribución**

   Envíe el paquete de instalación independiente del Agente de red al dispositivo seleccionado por cualquier método. Por ejemplo, puede copiar el paquete de instalación independiente en una unidad extraíble (como una unidad flash) o colocarlo en una carpeta compartida.

   En la ventana **Propiedades** del archivo del paquete de instalación independiente, verifique que el paquete de instalación independiente del Agente de red esté firmado por Kaspersky.

   Ejecute la instalación del paquete de instalación independiente del Agente de red en el dispositivo seleccionado. El Agente de red queda instalado de acuerdo con la configuración del paquete de instalación del Agente de red y se conecta al Servidor de administración. El dispositivo con el Agente de red se coloca en el grupo de administración que se especificó cuando se creó el paquete de instalación independiente del Agente de red.

   > Si se instala el Agente de red mediante un paquete de instalación independiente en un dispositivo que ejecuta Microsoft Windows XP Professional para sistemas integrados de 32 bits, la instalación falla. Para resolver este problema, instale primero la actualización KB2868626 para Windows XP desde el sitio web de Microsoft: https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

4. **Asignar el dispositivo con el Agente de red instalado para que funcione como punto de distribución.**

   Asigne el dispositivo con el Agente de red instalado para que funcione como punto de distribución.

5. **Configurar y realizar sondeos de red a través del punto de distribución**

   Configure el sondeo de red del punto de distribución que tiene el Agente de red instalado. Como opción, puede configurar el sondeo de red en la directiva del Agente de red.

   Después de completar el sondeo de red de acuerdo con el cronograma, los dispositivos clientes detectados se colocan en el grupo **Dispositivos no asignados**.

6. **Crear paquetes de instalación para el Agente de red y las aplicaciones administradas de Kaspersky**

   Si no abrió el asistente de inicio rápido u omitió el paso de crear paquetes de instalación, cree paquetes de instalación para las aplicaciones de Kaspersky. Debe crear paquetes de instalación, tanto para el Agente de red como para las aplicaciones administradas de Kaspersky, que sean apropiados para el sistema operativo instalado en los dispositivos cliente en la red de su organización.

7. **Eliminación de las aplicaciones de seguridad de terceros**

   Si en la red de su organización hay aplicaciones de seguridad de terceros instaladas en los dispositivos cliente, elimínelas antes de instalar las aplicaciones de Kaspersky.

8. **Instalación de aplicaciones de Kaspersky en dispositivos cliente**

   Cree tareas para instalar el Agente de red y las aplicaciones administradas de Kaspersky en dispositivos cliente en la red de su organización. Al crear las tareas, utilice el tipo de tarea **Instalar aplicación en remoto** Para la tarea de instalar el Agente de red, use la opción **Usando los recursos del sistema operativo mediante puntos de distribución**. Para la tarea de instalar aplicaciones administradas de Kaspersky, use la opción **Usando el Agente de red**. Después de crear las tareas, puede configurarlas. Asegúrese de que la programación de cada tarea cumpla con sus requisitos. Primero, se debe ejecutar la tarea que instalará el Agente de red. Después, tras instalar el Agente de red en los dispositivos de sus clientes, se debe ejecutar la tarea que instalará las aplicaciones administradas de Kaspersky.

Como opción, puede crear una tarea de instalación remota para instalar el Agente de red y las aplicaciones administradas de Kaspersky en los dispositivos cliente de la red de su organización. En este caso, en el bloque **Paquetes de instalación**, use la opción **Seleccionar paquete de instalación** y la opción **Seleccionar Agente de red**. En el bloque **Forzar la descarga del paquete de instalación**, use la opción **Usando los recursos del sistema operativo mediante puntos de distribución**.

También puede crear varias tareas de instalación remota para instalar las aplicaciones administradas de Kaspersky en diferentes grupos de administración o diferentes selecciones de dispositivos.

Si tiene dispositivos cliente que están fuera de la red con punto de distribución, por ejemplo, ordenadores portátiles de usuarios remotos, debe crear y entregar el Paquete de instalación independiente del Agente de red a esos dispositivos cliente por cualquier método. Instale el paquete de instalación independiente del Agente de red localmente en los dispositivos cliente. Luego, puede instalar las aplicaciones administradas de Kaspersky en los dispositivos de esos usuarios remotos siguiendo las mismas instrucciones que para otros dispositivos detectados por el punto de distribución.

Ejecute las tareas de instalación remota.

Como opción, para instalar las aplicaciones de Kaspersky, puede asistente de despliegue de la protección.

9. **Instalar Kaspersky Security for Mobile**

   Si planea administrar dispositivos móviles corporativos, siga las instrucciones que se brindan en la Ayuda de Kaspersky Security para dispositivos móviles. Allí encontrará información sobre el despliegue de Kaspersky Endpoint Security for Android.

10. **Verificación del despliegue inicial de las aplicaciones de Kaspersky**

    Genere y consulte el **Informe de versiones de la aplicación de Kaspersky**. Asegúrese de que las aplicaciones de Kaspersky administradas estén instaladas en todos los dispositivos cliente de su organización.

El cifrado de disco completo de Kaspersky Security Center Cloud Console solo admite BitLocker.

Crear paquetes de instalación para aplicaciones de Kaspersky.

Para desplegar las aplicaciones de Kaspersky en los dispositivos en red de su organización, debe crear paquetes de instalación de dichas aplicaciones en Kaspersky Security Center Cloud Console.

Para crear un paquete de instalación de la 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 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. Seleccione **Crear un paquete de instalación para una aplicación de Kaspersky**.

Aparece una lista de paquetes de distribución disponibles en los servidores web de Kaspersky.

4. Haga clic en el nombre de un paquete de distribución, por ejemplo, **Kaspersky Endpoint Security para Windows (<número de versión>)**.

   Se abrirá una ventana con información sobre el paquete de distribución.

5. Lea la información y haga clic en el botón **Descargar y crear paquete de instalación**.

   Si un paquete de distribución no se puede convertir automáticamente en un paquete de instalación, se mostrará el botón **Descargar el paquete de distribución** en lugar del botón **Descargar y crear paquete de instalación**. En este caso, descargue el paquete de distribución y luego use el archivo descargado para crear un paquete de instalación personalizado.

   Se inicia la descarga del paquete de instalación. Puede cerrar la ventana del asistente. En este caso, el proceso de descarga continuará en segundo plano. Puede rastrear el estado de descarga del paquete de instalación, así como filtrar y ordenar los estados en la columna **Estado del paquete**.

   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 paso 6 de las instrucciones. De manera predeterminada, los paquetes de instalación con estados **En curso** y **Aceptar EULA** se colocan al principio de la lista.

   Si planea realizar la migración de Kaspersky Security Center Web Console a Kaspersky Security Center Cloud Console y las regulaciones de seguridad de su organización requieren utilizar un proxy al acceder a la red corporativa, es posible que esto afecte el proceso de migración. Después de crear un paquete de instalación del Agente de red, debe especificar la configuración del proxy para garantizar la conexión entre las instancias del Agente de red en los dispositivos administrados y su espacio de trabajo de Kaspersky Security Center Cloud Console:

   a. Haga clic en el nombre del paquete de instalación.

   b. En la ventana de propiedades del paquete de instalación que se abre, vaya a la pestaña **Configuración**.

   c. Abra la sección **Conexión**.

   d. Seleccione la opción **Usar servidor proxy** y complete los campos **Dirección del servidor proxy** y **Puerto del servidor proxy**.

6. Para algunas aplicaciones de Kaspersky, durante el proceso de descarga, se muestra el botón **Mostrar el EULA**. Si ve este botón, haga lo siguiente:

   a. Haga clic en el botón **Mostrar el EULA** para leer el Contrato de licencia de usuario final (EULA).

   b. Lea el EULA que se muestra en la pantalla y haga clic en el botón **Aceptar**.

      La descarga continúa después de que acepte el EULA. Si hace clic en **Rechazar**, la descarga se detiene.

7. Cuando la descarga se haya completado, haga clic en el botón **Cerrar** (✕) para cerrar la ventana con información sobre el paquete de distribución.

Se ha creado el paquete de instalación. El paquete de instalación aparece en la lista de paquetes de instalación.

No es posible añadir un paquete de instalación con el mismo idioma de localización varias veces. Por ejemplo, si ya añadió el paquete de instalación de Kaspersky Endpoint Security para Windows (inglés), puede añadir paquetes de instalación de Kaspersky Endpoint Security para Windows localizados en otros idiomas, pero no en inglés.

Distribución de paquetes de instalación a servidores de administración secundarios

Para distribuir paquetes de instalación a servidores de administración secundarios:

1. Establezca conexión con el Servidor de administración que controla los servidores de administración secundarios pertinentes.

2. Utilizando uno de estos métodos, cree una tarea para distribuir los paquetes de instalación a los servidores de administración secundarios:

   - Si desea crear una tarea para los servidores de administración secundarios del grupo de administración seleccionado, inicie la creación de una tarea de grupo para ese grupo.

   - Si desea crear una tarea para servidores de administración secundarios específicos, inicie la creación de una tarea para dispositivos específicos.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones del asistente.

   En la ventana **Nueva tarea** del Asistente para crear nueva tarea, en el campo **Tipo de tarea** seleccione **Distribuir paquete de instalación**. También puede editar el nombre predeterminado de la tarea en el campo **Nombre de la tarea**.

   En el siguiente paso, especifique los Servidores de administración secundarios para la cobertura de la tarea y siga las instrucciones del Asistente para crear nueva tarea. El Asistente para crear nueva tarea creará la tarea de distribución de los paquetes de instalación seleccionados en los Servidores de administración secundarios específicos.

   > Cuando crea la tarea Distribuir paquete de instalación para Servidores de administración secundarios que se ejecutan localmente, la cobertura de la distribución (aparte de los paquetes de instalación personalizada) solo incluirá los paquetes de instalación de aplicaciones Kaspersky compatibles con Kaspersky Security Center Web Console que se ejecuta localmente, no importa qué opción de distribución haya seleccionado (**Todos los paquetes de instalación** o **Paquetes de instalación seleccionados**).

3. Ejecute la tarea manualmente o espere a que se inicie a consecuencia de la programación configurada para la tarea.

Los paquetes de instalación seleccionados se copiarán a los servidores de administración secundarios específicos.

Crear un paquete de instalación independiente para el Agente de red

Usted y los usuarios de dispositivos de su organización pueden utilizar paquetes de instalación independientes para instalar el Agente de red en dispositivos de forma local. Se pueden crear paquetes de instalación independientes para dispositivos con Windows, Linux o macOS.

> En Kaspersky Security Center Cloud Console, puede crear paquetes de instalación independientes solo para el Agente de red.

Un paquete de instalación independiente es un archivo ejecutable que se puede enviar por correo electrónico o transferir a un dispositivo cliente de otra manera. Este archivo recibido se puede ejecutar de manera local en el dispositivo cliente para instalar el Agente de red sin implicar a Kaspersky Security Center Cloud Console.

Para el Agente de red para Linux y el Agente de red para macOS, el paquete de instalación independiente es un archivo de script con la extensión .sh. Cuando ejecuta este archivo, el script desempaqueta el archivo adjunto que contiene el paquete de instalación y su configuración, y luego comienza la instalación.

Si se instala el Agente de red mediante un paquete de instalación independiente en un dispositivo que ejecuta Microsoft Windows XP Professional para sistemas integrados de 32 bits, la instalación falla. Para resolver este problema, instale primero la actualización KB2868626 para Windows XP desde el sitio web de Microsoft: https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

Para fines de autenticación, cada paquete de instalación independiente se firma con un certificado. El certificado se vuelve a emitir de vez en cuando. Después de cada procedimiento de reemisión del certificado, Kaspersky Security Center Cloud Console actualiza automáticamente las firmas de todos los paquetes de instalación independientes creados. Para los paquetes de instalación independientes descargados, no se puede realizar la actualización automática de firma. Por lo tanto, el certificado caduca y puede producirse un error de certificado cuando instale una aplicación desde un paquete de instalación independiente. En este caso, vuelva a descargar el paquete de instalación independiente.

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 los paquetes de instalación. Si el paquete de instalación del Agente de red no está en la lista, cree este paquete de instalación de forma manual.

2. En la lista de paquetes de instalación, haga clic en el nombre del paquete de instalación del Agente de red.

   Se muestra la ventana de propiedades del paquete de instalación del Agente de red.

3. Configure los ajustes del paquete de instalación del Agente de red, si es necesario, y cierre la ventana de propiedades del paquete de instalación del Agente de red.

4. 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.

5. 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.

6. Cerciórese de que la opción Instalar el **Instalar Agente de red junto con esta aplicación** esté activada 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.

7. En el paso **Mover a lista de dispositivos administrados**, la opción **No mover dispositivos** se selecciona de manera 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**.

8. Seleccione la opción **Abrir la lista de paquetes independientes** si desea que se muestre la lista de paquetes de instalación independientes una vez que el Asistente haya finalizado.

9. Haga clic en el botón **Finalizar**.

   Se cierra el Asistente para crear paquete de instalación independiente.

Se crea un paquete de instalación independiente del Agente de red. El paquete de instalación independiente creado se muestra en la lista de paquetes de instalación independientes que puede ver.

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:

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 los paquetes de instalación.

2. Haga clic en el botón **Ver la lista de paquetes independientes**, ubicado encima de la lista.

Se muestra una lista disponible de paquetes de instalación independientes.

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 del paquete de instalación del Agente de red**.
- **Versión del Agente de red**.
- **Tamaño**. Tamaño de archivo en megabytes (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.
- **Archivo hash**. La propiedad se utiliza para certificar que el paquete de instalación independiente no fue modificado por terceros 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:

- Descargar un paquete de instalación independiente a su dispositivo haciendo clic en el botón **Descargar**.

  Para fines de autenticación, cada paquete de instalación independiente se firma con un certificado. El certificado se vuelve a emitir de vez en cuando. Después de cada procedimiento de reemisión del certificado, Kaspersky Security Center Cloud Console actualiza automáticamente las firmas de todos los paquetes de instalación independientes creados. Para los paquetes de instalación independientes descargados, no se puede realizar la actualización automática de firma. Por lo tanto, el certificado caduca y puede producirse un error de certificado cuando instale una aplicación desde un paquete de instalación independiente. En este caso, vuelva a descargar el paquete de instalación independiente.

- Eliminar un paquete de instalación independiente haciendo clic en el botón **Eliminar**.

Crear un paquete de instalación personalizado

Puede utilizar paquetes de instalación personalizada para hacer lo siguiente:

- Para instalar cualquier aplicación (como un editor de texto) en un dispositivo cliente relacionado con Kaspersky Security Center Cloud Console, 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, incluido un archivo ejecutable. Una 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 opciones de línea de comandos, por ejemplo, para instalar la aplicación en modo silencioso.

No puede crear paquetes de instalación personalizados en el modo de prueba de Kaspersky Security Center Cloud Console.

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. Seleccione **Crear un paquete de instalación a partir de un archivo**.

4. Especifique el nombre del paquete de instalación y haga clic en el botón **Examinar**.

   Una ventana **Abrir** estándar le permite elegir un archivo de almacenamiento para crear el paquete de instalación.

5. Seleccione 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.

   Los archivos se descargan al Servidor de administración de Kaspersky Security Center Cloud Console.

   Si el Servidor de administración detecta que el archivo incluye una aplicación de Kaspersky, se muestra un mensaje de error. Puede descargar paquetes de instalación para las aplicaciones de Kaspersky desde los servidores web de Kaspersky. Esta operación está disponible si se selecciona **Operaciones → Aplicaciones de Kaspersky → Versiones actuales de la aplicación**.

6. Si el archivo comprimido seleccionado incluye varios archivos ejecutables, seleccione el que deba ejecutarse para instalar la aplicación utilizando el paquete de instalación creado.

7. Si lo desea, especifique los parámetros de 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. Consulte la documentación del proveedor de la aplicación para obtener detalles sobre los parámetros de línea de comandos.

   Se inicia la creación del paquete de instalación.

   El asistente le informa de la finalización del proceso.

   Si no se crea el paquete de instalación, se muestra un mensaje de error.

   En Kaspersky Security Center Cloud Console, el tamaño total de todos los paquetes de instalación en el Servidor de administración está limitado a 500 MB. Si en el proceso de creación de un paquete de instalación se supera el límite de tamaño total, elimine los paquetes de instalación creados anteriormente. El tamaño de un paquete de instalación se muestra en sus propiedades.

8. Haga clic en el botón **Finalizar** para cerrar el asistente.

El paquete de instalación personalizado que se creó se descarga en el 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, puede ver las siguientes propiedades de un paquete de instalación personalizado:

- **Nombre**. Nombre del paquete de instalación personalizado.
- **Estado del paquete**. Estado de descarga del paquete de instalación.
- **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 personalizado.
- **Sistema operativo**. Sistema operativo para el que se creó el paquete de instalación personalizado.
- **Creado**. Fecha de creación del paquete de instalación.
- **Modificado**. Fecha de modificación del paquete de instalación.
- **Tipo**. Aplicación de Kaspersky o aplicación de terceros.

En la lista de paquetes de instalación, al hacer clic en el enlace con el nombre de un paquete de instalación personalizado, puede cambiar los parámetros de línea de comandos y el nombre del paquete de instalación personalizado.

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.

Asimismo, es necesario que el punto de distribución tenga acceso a Internet y que siempre esté conectado.

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.

Ajustes del paquete de instalación del Agente de red

Para configurar un paquete de instalación del Agente de red, haga lo siguiente:

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 el enlace con el nombre del paquete de instalación del Agente de red.

   Se abrirá la ventana de propiedades del paquete de instalación del Agente de red seleccionado. La información de la ventana está agrupada en pestañas y secciones.

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**

- 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 casilla está marcada, todas las actualizaciones y parches descargados para el Agente de red se instalarán automáticamente.

  Si esta casilla no está marcada, todas las actualizaciones y los parches descargados se instalarán únicamente después de que cambie su estado a *Aprobado*. Las actualizaciones y los parches con el estado *Sin definir* no se instalarán.

  Esta casilla está activada de manera predeterminada.

Conexión

En esta sección, puede configurar la conexión del Agente de red al Servidor de administración:

- **Usar puerto UDP**

  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 activa esta opción, se añaden los puertos que el Agente de red utiliza a la lista de exclusiones del Firewall de Microsoft Windows.

Esta opción está habilitada de manera predeterminada.

- **No usar servidor proxy**
- **Usar servidor proxy**

  Dirección del servidor proxy

  Puerto del servidor proxy
- Autenticación del servidor proxy

  Si esta opción está activada, podrá especificar las credenciales de autenticación del servidor proxy en los campos de entrada.

  Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.

  Esta opción está deshabilitada de manera predeterminada.

  Nombre de usuario

  El nombre de usuario de la cuenta con la que se establece la conexión al servidor proxy.

  Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.

  Contraseña

  La contraseña de usuario de la cuenta con la que se establece la conexión al servidor proxy.

  Le recomendamos que utilice las credenciales de una cuenta que solamente tenga los privilegios mínimos necesarios para completar la autenticación ante el servidor proxy.

Por motivos de compatibilidad, no se recomienda especificar la configuración de conexión del proxy en la configuración del paquete de instalación del Agente de red.

Avanzado

En esta sección, puede configurar cómo se utilizan la puerta de enlace de conexión y la máquina virtual. También puede indicar si desea registrar a un usuario como propietario del dispositivo:

- **Conectar con el Servidor de administración usando una puerta de enlace de conexión**
- **Dirección de la puerta de enlace de conexión**
- 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.

- **Permitir ejecutar la utilidad del registro de usuarios después de la instalación del Agente de red**

  Si esta opción está activada, la utilidad de registro del usuario como propietario del dispositivo se ejecutará después de la instalación del Agente de red. Esta opción está deshabilitada de 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	✓	✓ * excepto la casilla de verificación **Abrir puertos del Agente de red en el Firewall de Microsoft Windows**	✓ * excepto la casilla de verificación **Abrir puertos del Agente de red en el Firewall de Microsoft Windows**
Avanzado	✓	✓	✓
Componentes adicionales	✓	✓	✓
Etiquetas	✓	✓ * excepto las reglas de etiquetado automático	✓ * excepto las reglas de etiquetado automático
Historial de revisiones	✓	✓	✓

Infraestructura virtual

Kaspersky Security Center Cloud Console admite el uso de máquinas virtuales. Para proteger su infraestructura virtual, debe instalar el Agente de red en cada máquina virtual.

Sugerencias sobre la reducción de la carga en máquinas virtuales

Al instalar el Agente de red en una máquina virtual, se le aconseja considerar desactivar algunas funciones de Kaspersky Security Center Cloud Console que parecen ser de poco uso para las 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 la Consola de administración.

Compatibilidad con máquinas virtuales dinámicas

Kaspersky Security Center Cloud Console admite 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. La máquina virtual con el Agente de red instalado también se añade a la base de datos del Servidor de administración. Después de que se apague esta máquina virtual, la entrada correspondiente también se debe eliminar de la base de datos del 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

Kaspersky Security Center Cloud Console admite la copia de una máquina virtual con el Agente de red instalado o la creación de una a partir de una plantilla con el Agente de red instalado.

El Agente de red puede detectar automáticamente la copia de máquinas virtuales en los siguientes casos:

- 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.

Uso del Agente de red para Windows, Linux y macOS: comparación

El Agente de red para macOS y Linux tiene varias limitaciones funcionales en comparación con el Agente de red para Windows. 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, macOS y Linux.

Comparación de funciones del Agente de red

Función del Agente de red	Windows	Linux	macOS
Instalación			
Instalación automática de las actualizaciones y los parches para el Agente de red	✓	—	—
Distribución automática de una clave	✓	✓	✓
Instalación manual, ejecutando el instalador de la aplicación en los dispositivos	✓	✓	✓
Sincronización forzada	✓	✓	✓
Punto de distribución			
Sondeo de red	✓ • Sondeo de intervalos IP • Sondeo de la red de Windows • Sondeo del controlador de dominio (Microsoft Active Directory)	✓ • Sondeo de intervalos IP • Sondeo del controlador de dominio (Microsoft Active Directory, Samba como 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	✓	✓	— Los puntos de distribución con macOS no pueden descargar actualizaciones de los servidores de actualizaciones de Kaspersky. Si hay uno o más dispositivos con macOS en el alcance de la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*, la tarea terminará con el estado *Error* aunque se complete sin errores en todos los dispositivos con Windows.
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.
Administración de aplicaciones de terceros			
Instalación remota de aplicaciones en los dispositivos	✓	—	—
Instalación de actualizaciones de software	✓	—	—
Configuración de actualizaciones del	✓	—	—

sistema operativo en una directiva del Agente de red			
Consulta de información sobre las vulnerabilidades de software	✓	—	—
Análisis de aplicaciones en busca de vulnerabilidades	✓	—	—
Inventariado del software instalado en los dispositivos	✓	✓	—
Máquinas virtuales			
Instalación del Agente de red en una máquina virtual	✓	✓	✓
Optimización de la configuración para infraestructuras de escritorios virtuales (VDI)	✓	✓	✓
Compatibilidad con máquinas virtuales dinámicas	✓	✓	✓
Otro			
Acciones de auditoría en dispositivos cliente remotos mediante Windows Desktop Sharing	✓	—	—
Administración del reinicio de los dispositivos	✓	—	—
Administrador de conexiones	✓	✓	✓
Conexión remota al escritorio de un dispositivo cliente	✓	—	—

Las siguientes secciones se muestran en las propiedades del punto de distribución, pero el Agente de red para macOS no es compatible con las funciones correspondientes:

- Origen de actualizaciones
- Servidor proxy de KSN
- Dominios de Windows
- Active Directory
- Intervalos IP
- Avanzado
- Estadísticas

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 Cloud Console 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 Cloud Console 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 Cloud Console utiliza el directorio especificado como directorio temporal para el acceso a través de SSH. La aplicación pondrá el paquete de instalación en este directorio e iniciará el procedimiento de instalación.

5. Haga clic en el botón **Guardar**.

   Se guardan los ajustes especificados en la tarea.

Reemplazo de aplicaciones de seguridad de terceros

La Instalación de aplicaciones de seguridad de Kaspersky a través de Kaspersky Security Center Cloud Console puede requerir la eliminación del software de terceros incompatible con la aplicación instalada. Kaspersky Security Center Cloud Console proporciona varias formas de eliminar las aplicaciones de terceros.

Eliminar aplicaciones incompatibles al configurar la instalación remota de una aplicación

Cuando esté configurando la instalación remota de una aplicación de seguridad, puede habilitar la opción **Desinstalar automáticamente las aplicaciones incompatibles**. Puede encontrar esta opción en el Asistente de despliegue de la protección. Cuando esta opción se activa, Kaspersky Security Center Cloud Console 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 las aplicaciones incompatibles, por medio de una tarea, 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, donde la otra tarea es **Desinstalar la aplicación de forma remota**.

Este método de desinstalación es útil cuando el instalador de la aplicación de seguridad no puede eliminar correctamente una aplicación incompatible.

Opciones para la instalación manual de aplicaciones

Puede instalar el Agente de red en dispositivos localmente sin involucrar a Kaspersky Security Center Cloud Console. Para hacer esto, cree un paquete de instalación independiente para el Agente de red como se describe en el siguiente tema: Creación de paquetes de instalación independientes. Transfiera el paquete a su dispositivo cliente e instálelo. Una vez completada la instalación del Agente de red, puede utilizar el dispositivo como punto de distribución.

Despliegue forzado con la tarea de instalación remota de Kaspersky Security Center Cloud Console

Para realizar el despliegue inicial del Agente de red u otras aplicaciones, puede forzar la instalación de los paquetes seleccionados mediante la tarea de instalación remota de Kaspersky Security Center Cloud Console, siempre que cada dispositivo tenga una cuenta de usuario con derechos de administrador local.

En el caso del despliegue inicial, el Agente de red no está instalado. Por lo tanto, en la configuración de la tarea de instalación remota, no se puede seleccionar la distribución de los archivos necesarios para la instalación de la aplicación mediante el Agente de red. Solo puede escoger distribuir archivos utilizando recursos del sistema operativo a través de puntos de distribución.

Debe especificar una cuenta que tenga acceso al recurso compartido admin$ en la configuración de la tarea de instalación remota.

Puede especificar dispositivos de destino explícitamente (con una lista), seleccionando el grupo de administración de Kaspersky Security Center Cloud Console al cual pertenecen o creando 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 activa en las propiedades de la tarea, la tarea se puede ejecutar inmediatamente después de que los dispositivos de destino se activen o cuando se muevan al grupo de administración de destino.

La instalación forzada consiste en la entrega de paquetes de instalación a dispositivos de destino, la copia posterior de archivos en el recurso admin$ en cada uno de los dispositivos de destino y el registro remoto de los servicios de compatibilidad en esos dispositivos. La entrega de paquetes de instalación a dispositivos de destino se realiza mediante una función de Kaspersky Security Center Cloud Console que garantiza la interacción de la red. Las condiciones siguientes se deben cumplir en este caso:

- Los dispositivos de destino son accesibles desde el lado del punto de distribución.
- La resolución del nombre para los dispositivos de destino funciona correctamente en la red.
- Los usos compartidos administrativos (admin$) permanecen activados en los dispositivos de destino.
- Los siguientes servicios del sistema se están ejecutando en los dispositivos de destino:
  - Servidor (LanmanServer)

De forma predeterminada, este servicio se está ejecutando.

- Iniciador de procesos del servidor DCOM (DcomLaunch)
- Asignador de endpoints de RPC (RpcEptMapper)
- Llamada a procedimiento remoto (RpcSs)

- El puerto TCP 445 está abierto en los dispositivos de destino para permitir el acceso remoto a través del Instrumental de administración de Windows.

  Los puertos TCP 139, UDP 137 y UDP 138 son utilizados por protocolos más antiguos y ya no son necesarios para las aplicaciones actuales.

  Se deben permitir puertos dinámicos de acceso saliente en el firewall para las conexiones desde los puntos de distribución a los dispositivos de destino.

- La configuración de seguridad de la directiva del dominio de Active Directory puede permitir el funcionamiento del protocolo NTLM durante el despliegue del Agente de Red.
- En los dispositivos de destino que ejecutan Microsoft Windows XP, el modo de uso compartido simple de archivos está deshabilitado.
- En los dispositivos de destino, el modelo de seguridad y uso compartido de acceso se configura como *Clásico: los usuarios locales se autentican como ellos mismos*. De ninguna manera puede ser *Solo invitados: los usuarios locales se autentican como invitados*.
- Los dispositivos de destino son miembros del dominio, o bien se crean cuentas uniformes con derechos de administrador en los dispositivos de destino de antemano.

Para desplegar correctamente el Agente de red u otras aplicaciones en un dispositivo que no está unido a un dominio de Active Directory de Windows Server 2003 o posterior, debe desactivar UAC remoto en ese dispositivo. UAC remoto es una de las razones que impide que las cuentas administrativas locales accedan a admin$, que es necesario para el despliegue forzado del Agente de red u otras aplicaciones. La desactivación del UAC remoto no afecta al UAC local.

Durante la instalación en dispositivos nuevos que todavía no se han asignado a ninguno de los grupos de administración de Kaspersky Security Center Cloud Console, puede abrir las propiedades de la tarea de instalación remota y especificar el grupo de administración al cual los dispositivos se moverán después de la instalación del Agente de red.

Al crear una tarea de grupo, tenga en cuenta que cada tarea de grupo afecta a todos los dispositivos en todos los grupos anidados dentro de un grupo seleccionado. Por lo tanto, debe evitar duplicar las tareas de instalación en los subgrupos.

Una manera sencilla de crear tareas para la instalación forzada de aplicaciones es la instalación automática. Para hacer esto, debe abrir las propiedades del grupo de administración, abrir la lista de paquetes de instalación y seleccionar 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.

Los dispositivos que actúan como puntos de distribución deben cumplir con los requisitos para los puntos de distribución. Debe asegurarse de que los puntos de distribución estén presentes en cada una de las subredes aisladas que alojan dispositivos de destino.

El espacio libre del disco en la partición con la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit debe superar, en gran cantidad, el tamaño total de los paquetes de distribución de aplicaciones instaladas.

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**.

Paso 1. Iniciar Asistente de despliegue de la protección

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 la forma en que desea instalar el paquete de instalación seleccionado:

- **Instalación remota por Kaspersky Security Center**
- **Instalación remota por API de Microsoft Azure**

Luego, 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. 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 3. 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 4. Configurar la tarea de instalación remota

En la página de la configuración de la tarea "**Instalación remota**", especifique la configuración para la instalación remota de la aplicación.

En el grupo de ajustes **Forzar la descarga del paquete de instalación**, especifique cómo los archivos necesarios para la instalación de la aplicación se distribuyen a los dispositivos cliente:

- **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.

Está opción se habilita de manera predeterminada para las tareas de instalación remota creadas en servidores de administración virtuales.

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.

Contraseña para desinstalar la aplicación de Kaspersky actual

El campo **Contraseña para desinstalar la aplicación de Kaspersky actual** solo está disponible si ha seleccionado la opción **Usando el Agente de red** en el grupo de configuración **Forzar la descarga del paquete de instalación**.

Introduzca la contraseña en el campo **Contraseña para desinstalar la aplicación de Kaspersky actual** si migra de una aplicación de Kaspersky a otra y su aplicación actual está protegida con contraseña. Tenga en cuenta que durante la migración, se desinstalará su aplicación de Kaspersky actual.

Para completar el escenario de migración correctamente, asegúrese de que se cumplan los siguientes requisitos previos:

- Está utilizando el Agente de red de Kaspersky Security Center 14.2 for Windows o una versión posterior.
- Está instalando la aplicación en dispositivos que ejecutan Windows.

Paso 5. Opciones de reinicio

Indique qué acción se llevará a cabo si se necesita reiniciar el sistema operativo al instalar la aplicación:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o 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)**

    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.

  - **Reiniciar después de (min)**

    Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

    Esta opción está 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.

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 Cloud Console 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)**

  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 asigna la tarea de instalación remota. En este caso, puede especificar una cuenta de usuario o un certificado SSH para instalar la aplicación.

- **Cuenta local**. Si se selecciona esta opción, especifique la cuenta bajo la que se ejecutará el instalador de aplicación. Haga clic en el botón **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.

- **Certificado SSH**. Si desea instalar una aplicación en un dispositivo cliente basado en Linux, puede especificar un certificado SSH en lugar de una cuenta de usuario. Haga clic en el botón **Añadir**, seleccione **Certificado SSH** y, a continuación, especifique las claves pública y privada del certificado.

  Para generar una clave privada, puede utilizar la utilidad ssh-keygen. Tenga en cuenta que Kaspersky Security Center Cloud Console admite el formato PEM de claves privadas, pero la utilidad ssh-keygen genera claves SSH en formato OPENSSH de manera predeterminada. El formato OPENSSH no es compatible con Kaspersky Security Center Cloud Console Para crear una clave privada en el formato PEM admitido, agregue la opción -m PEM en el comando ssh-keygen. Por ejemplo:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "< correo electrónico del usuario >"
  ```

Paso 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 la 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.

Configuración de la red para interactuar con servicios externos

Kaspersky Security Center Cloud Console utiliza la siguiente configuración de red para interactuar con los servicios externos.

Configuración de red

Configuración de red	Dirección	Descripción
Puerto: 443 Protocolo: HTTPS	activation-v2.kaspersky.com/activationservice/activationservice.svc	Activación de la aplicación.
Puerto: 443 Protocolo: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com	Actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky.

	https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	
Puerto: 443 Protocolo: HTTPS	https://downloads.upd.kaspersky.com	• Actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky. • Comprobar si se puede acceder a los servidores de Kaspersky. Antes de descargar las bases de datos y los módulos de software de Kaspersky, Kaspersky Security Center Cloud Console 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.
Puerto: 80 Protocolo: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com	Actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky.

	http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	
Puerto: 443 Protocolo: HTTPS	ds.kaspersky.com	Usar Kaspersky Security Network.
Puerto: 443, 1443 Protocolo: HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Usar Kaspersky Security Network.
Protocolo: HTTPS	click.kaspersky.com redirect.kaspersky.com	Seguir los enlaces desde la interfaz.
Puerto: 80 Protocolo: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Infraestructura de clave pública (PKI).
Puerto: 443 Protocolo: HTTPS	https://ipm-klca.kaspersky.com	Anuncios de marketing.

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 Cloud Console 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.

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.

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 (para Ubuntu 10.04, la versión de Sudo 1.7.2p1 o posterior)
   - 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 que ha abierto, añada la siguiente línea al final del archivo: `username > 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` 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.

6. Si desea instalar el Agente de Red en dispositivos que utilicen el sistema operativo RED OS 7.3.4 o posterior, o MSVSPHERE 9.2 o posterior, instale el paquete libxcrypt-compat para el correcto funcionamiento del Agente de Red.

Instalación remota del Agente de red

Para instalar el Agente de red en dispositivos Linux de manera remota:

1. Descargue y cree un paquete de instalación:

a. Antes de iniciar la instalación del paquete en el dispositivo, asegúrese de que ya tiene instaladas todas las dependencias (programas y bibliotecas) para este paquete.

Puede ver las dependencias de cada paquete por su propia cuenta, mediante las utilidades específicas de la distribución Linux en la que se instalará el paquete. Para obtener más información sobre las utilidades, consulte la documentación de su sistema operativo.

b. 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:

- klnagent.kpd
- akinstall.sh
- Paquete .deb o .rpm de Agente de red

2. Cree una tarea de instalación remota con la configuración siguiente:

- En la página **Configuración** del Asistente para crear nueva tarea, 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`.

Instalar aplicaciones mediante una tarea de instalación remota

Kaspersky Security Center Cloud Console permite que usted instale aplicaciones en dispositivos remotamente, usando las tareas de instalación remotas. Estas tareas se crean y se asignan a dispositivos a través de un asistente dedicado. Para asignar una tarea de modo más fácil y rápido, puede especificar dispositivos (hasta 1000) 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**. En este caso, 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 evitar problemas que puedan ocurrir durante la instalación de la aplicación en un dispositivo cliente sin Agente de red instalado, debe proceder como se describe en el despliegue forzado a través de la tarea de instalación remota de Kaspersky Security Center Cloud Console.

Instalación de una aplicación de forma remota

Este artículo 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.

     Si se asigna una tarea a un grupo de administración, la pestaña **Seguridad** no se muestra en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

   - Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista

     Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

     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:

   - Seleccione cómo desea instalar la aplicación seleccionada:

     - **Instalación remota por Kaspersky Security Center**
     - **Instalación remota por API de Microsoft Azure**

       Para obtener más información sobre cómo instalar aplicaciones en máquinas virtuales de Microsoft Azure, consulte Instalación remota de aplicaciones en máquinas virtuales de Azure.

- 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.

    Está opción se habilita de manera predeterminada para las tareas de instalación remota creadas en servidores de administración virtuales.

- 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 Cloud Console 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** y reinicie la tarea. O bien, puede crear una nueva tarea *Instalar aplicación de forma remota*.

- Si migra de una aplicación de Kaspersky a otra y su aplicación actual está protegida con contraseña, introduzca la contraseña en el campo **Contraseña para desinstalar la aplicación de Kaspersky actual**. Tenga en cuenta que durante la migración, se desinstalará su aplicación de Kaspersky actual.

  El campo **Contraseña para desinstalar la aplicación de Kaspersky actual** solo está disponible si ha seleccionado la opción **Usando el Agente de red** en el grupo de configuración **Forzar la descarga del paquete de instalación**.

  Puede usar la contraseña de desinstalación solo para la migración de Kaspersky Security para Windows Server a Kaspersky Endpoint Security para Windows al instalar Kaspersky Endpoint Security para Windows mediante la tarea *Instalar aplicación de forma remota*. El uso de la contraseña de desinstalación al instalar otras aplicaciones puede provocar errores de instalación.

Para completar el escenario de migración correctamente, asegúrese de que se cumplan los siguientes requisitos previos:

- Está utilizando el Agente de red de Kaspersky Security Center 14.2 para Windows o una versión posterior.
- Está instalando la aplicación en dispositivos con Windows.

- Defina las opciones adicionales:
  - **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 Cloud Console 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 Cloud Console 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.

  La opción **No mover dispositivos** está seleccionada de manera 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.

   - **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.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está 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.

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 este caso, puede especificar una cuenta de usuario o un certificado SSH para instalar la aplicación.

- **Cuenta local**. Si se selecciona esta opción, especifique la cuenta bajo la que se ejecutará el instalador de aplicación. Haga clic en el botón **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.

- **Certificado SSH**. Si desea instalar una aplicación en un dispositivo cliente basado en Linux, puede especificar un certificado SSH en lugar de una cuenta de usuario. Haga clic en el botón **Añadir**, seleccione **Certificado SSH** y, a continuación, especifique las claves pública y privada del certificado.

  Para generar una clave privada, puede utilizar la utilidad ssh-keygen. Tenga en cuenta que Kaspersky Security Center Cloud Console admite el formato PEM de claves privadas, pero la utilidad ssh-keygen genera claves SSH en formato OPENSSH de manera predeterminada. El formato OPENSSH no es compatible con Kaspersky Security Center Cloud Console Para crear una clave privada en el formato PEM admitido, agregue la opción -m PEM en el comando ssh-keygen. Por ejemplo:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "< correo electrónico del usuario >"
  ```

9. En el paso **Finalizar la creación de 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.

Inicio y detención de aplicaciones de Kaspersky

Puede usar la tarea *Iniciar o detener aplicación* para iniciar y detener aplicaciones de Kaspersky en dispositivos administrados.

Para crear la tarea Iniciar o detener la aplicación:

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 crear la tarea.
4. En la lista **Tipo de tarea**, seleccione la tarea **Activación de aplicaciones**.
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.
7. En la ventana **Aplicaciones**, haga lo siguiente:

   - Seleccione las casillas de verificación junto a los nombres de las aplicaciones para las que desea crear la tarea.
   - Seleccione la opción **Iniciar aplicación** o **Detener aplicación**.
8. Si desea modificar la configuración predeterminada de la tarea, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en el paso **Finalizar la creación de tareas**. 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, especifique la configuración general de la tarea que se ajuste a sus necesidades y luego guarde la configuración.

La tarea queda creada y configurada.

Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

Administración de dispositivos móviles

La administración de la protección de dispositivos móviles a través de Kaspersky Security Center Cloud Console se realiza mediante la función de administración de dispositivos móviles. Habilite y configure la característica Administración de dispositivos móviles si planea administrar dispositivos móviles que pertenezcan a los empleados de su organización.

Podrá usar las funciones de Administración de dispositivos móviles para gestionar los dispositivos Android del personal. La protección la proporciona la app Kaspersky Endpoint Security for Mobile instalada en los dispositivos. Esta app móvil garantiza la protección de los dispositivos móviles contra las amenazas web, los virus y otros programas que representan amenazas.

Dispositivos iOS

Kaspersky Device Management for iOS garantiza la protección y el control de los dispositivos móviles que están conectados a Kaspersky Security Center Cloud Console.

La app Kaspersky Security for iOS ofrece las siguientes funciones clave:

- **Protección web**. Este componente bloquea los sitios web maliciosos diseñados para propagar códigos maliciosos. La Protección web también bloquea los sitios web falsos (phishing) diseñados para robar datos confidenciales del usuario (por ejemplo, contraseñas para sistemas bancarios en línea o de dinero electrónico) y acceder a la información financiera del usuario.

- **Detección de Jailbreak**. Cuando Kaspersky Security for iOS detecta un jailbreak, muestra un mensaje de suceso crítico y le informa sobre el problema.

Para obtener información sobre el despliegue de la protección y la administración de dispositivos móviles, consulte la Ayuda de Kaspersky Security para dispositivos móviles.

Capacidades de detección y respuesta

Esta sección contiene información sobre las soluciones de Kaspersky que se pueden integrar en Kaspersky Security Center Cloud Console para añadir las capacidades de detección y respuesta a la consola.

Acerca de las capacidades de detección y respuesta

Kaspersky Security Center Cloud Console puede integrar funciones de otras soluciones de Kaspersky en la interfaz de la consola. Por ejemplo, puede añadir las funciones de detección y respuesta a la funcionalidad de Kaspersky Security Center Cloud Console.

Las soluciones de detección y respuesta están diseñadas para proteger la infraestructura de TI de una organización frente a ciberamenazas complejas. La funcionalidad de las soluciones combina la detección automática de amenazas con la capacidad de responder a ellas para luchar contra ataques complejos, incluidos nuevos exploits, ransomware, ataques sin archivos y métodos que utilizan herramientas legítimas del sistema.

Puede integrar las siguientes soluciones:

- Kaspersky Endpoint Detection and Response Optimum

  Después de que una aplicación de Kaspersky Endpoint Protection Platform (también conocida como EPP) detecta una amenaza, Kaspersky Security Center Cloud Console añade una nueva alerta a la lista de alertas. Una alerta contiene información detallada sobre la amenaza detectada y le permite analizar e investigar la amenaza. Además, puede visualizar la amenaza creando un gráfico con la cadena de desarrollo de la amenaza. El gráfico describe las etapas de despliegue del ataque detectado a tiempo.

  Como respuesta, puede elegir una de las acciones de respuesta predefinidas, por ejemplo, aislar un objeto que no es de confianza, aislar un dispositivo comprometido de la red o crear una regla de prevención de ejecución para un objeto que no es de confianza.

  Para obtener información sobre la activación de la solución, consulte la documentación de Kaspersky Endpoint Detection and Response Optimum.

- Kaspersky Managed Detection and Response

  Después de que una aplicación de Kaspersky EPP detecta una amenaza, Kaspersky Security Center Cloud Console añade un nuevo incidente a la lista de incidentes. Un incidente contiene información detallada sobre la amenaza detectada. Los analistas del Centro de Operaciones de Seguridad (SOC) de MDR de Kaspersky o de una empresa externa investigan los incidentes y ofrecen respuestas para resolverlos. Puede aceptar o rechazar las medidas ofrecidas de forma manual o activar la opción para aceptar todas las respuestas automáticamente.

  Para obtener información sobre la activación de la solución, consulte la documentación de Kaspersky Managed Detection and Response.

- Kaspersky Endpoint Detection and Response Expert

  Esta es una solución para organizaciones que tienen un equipo de analistas del SOC. Las amenazas detectadas se registran como alertas o incidentes que se pueden asignar a los analistas del SOC para que realicen una investigación. Kaspersky Endpoint Detection and Response Expert proporciona información detallada sobre cada alerta o incidente, así como las herramientas para administrar alertas e incidentes, buscar amenazas y desarrollar reglas personalizadas. Los analistas del SOC o los directores de seguridad pueden seleccionar manualmente las acciones de respuesta, o se pueden implementar las acciones de respuesta automatizadas predefinidas.

  Para obtener información sobre la activación de la solución, consulte la documentación de Kaspersky Endpoint Detection and Response Expert.

Cambios en la interfaz después de integrar las funciones de detección y respuesta

Las siguientes soluciones de Kaspersky proporcionan funciones de detección y respuesta que se pueden integrar en la interfaz de Kaspersky Security Center Cloud Console:

- Kaspersky Endpoint Detection and Response (EDR) Optimum
- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response (EDR) Expert

La siguiente tabla enumera los cambios que las soluciones realizan en la interfaz de Kaspersky Security Center Cloud Console tras la integración.

Cambios en la interfaz realizados a través de las soluciones integradas de Kaspersky

Solución	Cambios en Kaspersky Security Center Cloud Console
Kaspersky EDR Optimum	Añade los siguientes elementos: • Sección **Alertas** (**Control e informes** → **Alertas**). Las alertas detectadas por esta solución se enumeran en la pestaña **Optimum**. • Un widget en **Panel** (**Control e informes** → **Panel**).
Kaspersky MDR	Añade los siguientes elementos: • Sección **MDR** (**Control e informes** → **MDR**). • La opción **Mostrar las funciones de MDR** (**Configuración** → **Opciones de interfaz** → **Mostrar las funciones de MDR**). • Un widget en **Panel** (**Control e informes** → **Panel**).
Kaspersky EDR Expert	Añade los siguientes elementos: • Sección **Alertas** (**Control e informes** → **Alertas**). Las alertas detectadas por esta solución se enumeran en la pestaña **Experto**. • Sección **Incidentes** (**Control e informes** → **Incidentes**). • Sección **Búsqueda de amenazas** (**Control e informes** → **Búsqueda de amenazas**). • Sección **Reglas personalizadas** (**Control e informes** → **Reglas personalizadas**). • Configuración general de Kaspersky EDR Expert (**Configuración** → **Integración** → **Kaspersky EDR Expert**). • Widgets en **Panel** (**Control e informes** → **Panel**).

Descubrir dispositivos en red y crear grupos de administración

En esta sección se describe la búsqueda y el descubrimiento de dispositivos en red, además de la creación de grupos de administración para esos dispositivos.

Kaspersky Security Center Cloud Console 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 detección permite encontrar los siguientes dispositivos:

- Dispositivos administrados en grupos de administración del Servidor de administración de Kaspersky Security Center Cloud Console y sus Servidores de administración secundarios.
- Dispositivos no asignados administrados por el Servidor de administración de Kaspersky Security Center Cloud Console y sus Servidores de administración secundarios.

Escenario: Descubrir dispositivos conectados a la red

Debe realizar la detección de dispositivos antes del despliegue inicial de las aplicaciones de seguridad. Cuando se detecten todos los dispositivos en red, puede obtener información sobre ellos y administrarlos a través de directivas. Se necesitan sondeos de red regulares para detectar si hay dispositivos nuevos y si los dispositivos detectados todavía están en la red.

Cuando finaliza el escenario, la detección de dispositivos está configurada y se llevará a cabo de acuerdo con la programación especificada.

Requisitos previos

En Kaspersky Security Center Cloud Console, la detección de dispositivos se realiza mediante puntos de distribución. Antes de comenzar, haga lo siguiente:

- Decida qué dispositivos actuarán como puntos de distribución.
- Instale Agentes de red en los dispositivos que elija.
- Designe manualmente los dispositivos que funcionarán como puntos de distribución.

Etapas

El escenario avanza en etapas:

1. **Elegir tipos de descubrimiento**

   Decida qué tipo(s) de descubrimiento desea utilizar regularmente.

2. **Configurar sondeos**

   En las propiedades de cada punto de distribución, active y configure los tipos de sondeo de red que escoja: Sondeo de red de Windows, Sondeo del controlador de dominio, o Sondeo de rango de IP. Asegúrese de que la programación de sondeos satisfaga las necesidades de su organización.

   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)**

   Los nuevos dispositivos que aparezcan en su red, se detectan durante sondeos regulares y se incluyen automáticamente en el grupo **Dispositivos no asignados**. Si lo desea, puede configurar las reglas para el traslado automático de estos dispositivos al grupo **Dispositivos administrados**. También puede definir reglas de retención.

   Si omite este paso que configura la regla, todos los dispositivos recién detectados van al grupo **Dispositivos no asignados** y se quedan allí. Si lo desea, puede mover estos dispositivos al grupo de **Dispositivos administrados** manualmente. Si mueve los dispositivos al grupo de **Dispositivos administrados** manualmente, puede analizar la información sobre cada dispositivo y decidir si desea moverlo a un grupo de administración y, de ser así, a qué grupo.

Cuando se completa una operación de sondeo de red, verifique que los dispositivos recién descubiertos estén organizados de acuerdo con las reglas configuradas. Si no se configura ninguna regla, los dispositivos se quedan en el grupo **Dispositivos no asignados**.

Sondeo de red

Kaspersky Security Center Cloud Console recibe información sobre la estructura de red y los dispositivos en esta red a través de encuestas periódicas de la red de Windows, los rangos de IP, el controlador de dominio Microsoft Active Directory y el controlador de dominio Samba. Para un controlador de dominio Samba, se utiliza Samba 4 como controlador de dominio Active Directory. El sondeo de la red puede iniciarse manualmente o automáticamente de acuerdo con una programación.

Según los resultados de esta encuesta, Kaspersky Security Center Cloud Console actualiza la lista de dispositivos no asignados. También puede configurar reglas para que los nuevos dispositivos descubiertos se muevan automáticamente a los grupos de administración.

Kaspersky Security Center Cloud Console utiliza los siguientes métodos de sondeo de red:

- *Sondeo de rangos IP*. Kaspersky Security Center Cloud Console sondea los rangos IP especificados utilizando paquetes de Protocolo de control de mensajes de Internet (ICMP, por sus siglas en inglés) y recopila un conjunto completo de datos en los dispositivos de esos rangos IP.

- *Sondeo de la red de Windows*. Puede ejecutar cualquiera de las dos encuestas de red de Windows: rápida o completa. Durante un sondeo rápido, Kaspersky Security Center Cloud Console únicamente recopilará la información de los dispositivos de la lista de nombre NetBIOS de todos los dominios y grupos de trabajo de la red. Durante una encuesta completa, se solicita la siguiente información de cada dispositivo: nombre del sistema operativo (SO), dirección IP, nombre DNS y nombre NetBIOS.

- *Sondeo de controladores de dominio*. La información sobre la estructura de la unidad de Active Directory y sobre los nombres DNS de los dispositivos de los grupos de Active Directory se registra en la base de datos de Kaspersky Security Center Cloud Console.

Los resultados del sondeo se muestran en la sección **Detección y despliegue → Detección** por separado para el *sondeo de red de Windows* y los métodos de *sondeo de los controladores de dominio*.

Los resultados del sondeo para el método *de sondeo de rango de IP* se muestran en la sección **Detección y despliegue → Dispositivos no asignados**.

Se puede mostrar un dispositivo en más de un área de detección. Si se detecta un dispositivo en el dominio HQ y su dirección es 192.168.0.1, el dispositivo aparecerá tanto en la sección **Dominios de Windows** como en la sección **Dispositivos no asignados**. Puede modificar la configuración de sondeo de red para cada método de sondeo. Por ejemplo, puede cambiar la frecuencia con la que se realizan los sondeos o definir si el sondeo de Active Directory alcanzará a todo el bosque o estará limitado a un dominio específico.

Sondeo de la red de Windows

Acerca del sondeo de la red de Windows

Cuando se realiza un sondeo rápido, el Servidor de administración solo recupera información de la lista de nombres NetBIOS correspondientes a los dispositivos de todos los dominios y grupos de trabajo de la red. Cuando se realiza un sondeo completo, se solicita la siguiente información a cada dispositivo cliente:

- Nombre del sistema operativo
- Dirección IP
- Nombre DNS
- Nombre NetBIOS

Para realizar un sondeo rápido o completo, se deben cumplir los siguientes requisitos:

- UDP de Puertos 137/138, TCP 139 debe estar disponible en la red.
- Se debe utilizar el servicio Explorador de equipos de Microsoft y el equipo del explorador principal debe estar activado en el punto de distribución.
- Se debe utilizar el servicio Explorador de equipos de Microsoft y el equipo explorador principal debe estar habilitado en esta cantidad de dispositivos cliente:
  - al menos un dispositivo si no hay más de 32 dispositivos conectados a la red;
  - al menos un dispositivo por cada 32 dispositivos conectados a la red.

Para realizar un sondeo completo, primero debe haberse realizado al menos un sondeo rápido.

Cómo ver y modificar la configuración del sondeo de la red de Windows

Para modificar las propiedades del sondeo de la red de Windows:

1. En el menú principal, 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 que desea usar para sondear la red.

   Se abre la ventana de propiedades del punto de distribución.

4. Seleccione la sección **Sondeo de dominios de Windows**.
5. Utilizando el interruptor **Activar sondeo de red**, habilite o deshabilite el sondeo de la red de Windows.
6. Configure la programación para el sondeo rápido y el sondeo completo.

7. Haga clic en el botón **Aceptar**.

Las propiedades se guardan y se aplican a todos los dominios y grupos de trabajo de Windows descubiertos.

Sondeo del controlador de dominio

Kaspersky Security Center Cloud Console admite el sondeo de un controlador de dominio de Microsoft Active Directory y un controlador de dominio Samba a través de un punto de distribución.

Kaspersky Security Center Cloud Console le permite sondear un controlador de dominio Samba solo mediante el uso de un punto de distribución de Linux. Para un controlador de dominio Samba, se utiliza Samba 4 como controlador de dominio Active Directory.

Cuando sondea un controlador de dominio, 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. El sondeo del controlador de dominio se realiza de acuerdo a la programación que configure.

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 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. Elija 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 las reglas de movimiento de dispositivos, los dispositivos recién descubiertos se incluyen automáticamente en el grupo **Dispositivos administrados**. Si no se han habilitado reglas de movimiento, los dispositivos recién descubiertos se incluyen automáticamente en el grupo **Dispositivos no asignados**.

Las cuentas de usuario detectadas se pueden utilizar para la autenticación de dominio en Kaspersky Security Center Cloud Console.

Visualización de los resultados del sondeo del controlador de dominio

Para ver los resultados del sondeo del controlador de dominio, haga lo siguiente:

1. En el menú principal, vaya a **Detección y despliegue** → **Detección** → **Controladores de dominio**.

   Se muestra la lista de unidades organizativas descubiertas.

2. Seleccione una unidad organizativa y luego haga clic en el botón **Dispositivos**.

   Se muestra la lista de dispositivos incluidos en la unidad organizativa.

Puede hacer búsquedas en la lista y filtrar los resultados.

Sondeo de intervalos IP

Kaspersky Security Center Cloud Console intenta realizar una resolución de nombres inversa para cada dirección 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 Cloud Console. 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. En las redes donde se utiliza Active Directory, esta zona se mantiene automáticamente. Pero en estas redes, el sondeo de subred IP no proporciona más información que el sondeo de Active Directory. Además, quienes administran una red pequeña rara vez configuran la zona de búsqueda inversa, pues no todos los servicios de red la necesitan para operar. Por estos motivos, el sondeo de subredes IP está deshabilitado de forma predeterminada.

Inicialmente, Kaspersky Security Center Cloud Console obtiene rangos de IP para el sondeo desde la configuración de red del dispositivo del punto de distribución que se utiliza para sondeo de red. Si la dirección del dispositivo es 192.168.0.1 y la máscara de subred es 255.255.255.0, Kaspersky Security Center Cloud Console incluye automáticamente la red 192.168.0.0/24 en la lista de direcciones del sondeo. Kaspersky Security Center Cloud Console sondea todas las direcciones desde 192.168.0.1 hasta 192.168.0.254.

No se recomienda usar el sondeo de intervalos IP si ya se utilizan los métodos de sondeo de la red de Windows o de sondeo de Active Directory.

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, 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 que desea usar para sondear la red.

   Se abre la ventana de propiedades del punto de distribución.

4. Seleccione la sección **Sondeo de rangos IP**.

5. Utilizando el interruptor **Activar sondeo del rango**, habilite o deshabilite el sondeo de intervalos IP.

6. Configurar la programación del sondeo. De forma predeterminada, el sondeo de intervalos IP se ejecuta cada 420 minutos (7 horas).

7. Si es necesario, añada o modifique los rangos de IP para sondear.

   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.

8. Haga clic en el botón **Aceptar**.

Las propiedades se guardan y se aplican a todos los intervalos IP.

Configuración de un controlador de dominio Samba

Kaspersky Security Center Cloud Console 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 garantiza la interacción correcta entre Kaspersky Security Center Cloud Console 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 `netbios name` y los parámetros del `workgroup` en el archivo /etc/samba/smb.conf.

Agregar y modificar un intervalo IP

Inicialmente, Kaspersky Security Center Cloud Console obtiene rangos de IP para el sondeo desde la configuración de red del dispositivo del punto de distribución que se utiliza para sondeo de red. Si la dirección del dispositivo es 192.168.0.1 y la máscara de subred es 255.255.255.0, Kaspersky Security Center Cloud Console incluye automáticamente la red 192.168.0.0/24 en la lista de direcciones del sondeo. Kaspersky Security Center Cloud Console 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.

Para agregar un nuevo intervalo IP:

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 que desea usar para sondear la red.

   Se abre la ventana de propiedades del punto de distribución.

4. Seleccione la sección **Sondeo de rangos IP**.

5. Para agregar un nuevo intervalo IP, haga clic en el botón **Añadir**.

6. En la ventana que se abre, defina los siguientes ajustes:

   - **Nombre**

     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. 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.

   - **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.

7. Haga clic en el botón **Aceptar**.

   El nuevo intervalo IP se agrega a la lista de intervalos IP.

Cuando se complete el sondeo, haga clic en el botón **Dispositivos** para ver la lista de dispositivos descubiertos. De forma predeterminada, los resultados del sondeo serán válidos por veinticuatro horas (el mismo tiempo por el que se considera vigente una dirección IP).

Ajuste de puntos de distribución y puertas de enlace de conexión

Una estructura de grupos de administración en Kaspersky Security Center Cloud Console realiza las funciones siguientes:

- Define el alcance de las directivas

  Existe otra forma de aplicar ajustes pertinentes en dispositivos: mediante el uso de *perfiles de directiva*. En este caso, el alcance de las directivas está configurado con etiquetas, ubicaciones del dispositivo en unidades organizacionales de Active Directory, membrecía en grupos de seguridad de Active Directory, etc.

- 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.

- Configura los derechos de acceso a dispositivos y Servidores de administración secundarios

- 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 los puntos de distribución le permite ahorrar tráfico de 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.

Cálculo de la cantidad de puntos de distribución y su configuración

Cuantos más dispositivos cliente contiene una red, más puntos de distribución se requieren. Use las tablas a continuación para calcular la cantidad de puntos de distribución necesarios para su red.

Compruebe que los dispositivos que planea usar como 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

Si un punto de distribución no está disponible, actualice las bases de datos, los módulos de software y las aplicaciones de Kaspersky manualmente o directamente desde los servidores de actualización de Kaspersky.

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:

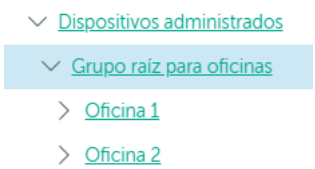
- Armar la estructura de grupos de administración tomando en cuenta la topología de la red. No es necesario que la estructura de grupos de administración refleje con absoluta precisión la topología de la red. Es suficiente con que haya coincidencia entre las partes independientes de la red y ciertos grupos de administración.

- Armar la estructura de grupos de administración sin tener en cuenta la topología de la red. En este caso, debe asignar uno o varios dispositivos para que actúen como puntos de distribución para un grupo de administración de raíz 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 la misma cobertura que abarca a 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.

Designación manual de puntos de distribución

Kaspersky Security Center Cloud Console le permite asignar manualmente dispositivos para actuar como puntos de distribución. Recomendamos que calcule la cantidad y la configuración de los puntos de distribución necesarios para su red.

Los puntos de distribución con macOS no pueden descargar actualizaciones de los servidores de actualizaciones de Kaspersky.

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

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. Haga clic en el botón **Asignar**.

4. 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.

5. Seleccione el grupo de administración que desee incluir en el alcance del punto de distribución seleccionado.

6. Haga clic en el botón **Añadir**.

El punto de distribución agregado aparecerá en la lista de puntos de distribución, en la sección **Puntos de distribución**.

7. Seleccione el punto de distribución recién añadido en la lista para abrir su ventana de propiedades.

8. En la ventana de propiedades, configure los ajustes del punto de distribución:

   - La sección **General** contiene la configuración de interacción entre el punto de distribución 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 Cloud Console 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.

     - 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 Cloud Console, un punto de distribución puede funcionar como servidor push para dispositivos basados en Windows y Linux administrados por el Agente de red. 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 al mismo grupo de administración, puede habilitar un 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 **Cobertura**, especifique el ámbito en el que el punto de distribución distribuirá actualizaciones (grupos de administración y/o ubicación de la red).

  Para que un dispositivo pueda determinar su ubicación de red, debe tener un sistema operativo Windows. No se puede determinar la ubicación de red de dispositivos con otros sistemas operativos.

- 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.

  Esta característica no es compatible con dispositivos de puntos de distribución que ejecuten Linux o macOS.

  El punto de distribución enviará a Kaspersky las estadísticas de KSN que se enumeran en la declaración de Kaspersky Security Network. De forma predeterminada, la declaración de KSN se encuentra en %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Esta opción está deshabilitada de manera predeterminada. Esta opción solo se activa si la opción **Acepto usar Kaspersky Security Network** está activada 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.

- Configure los sondeos de los dominios de Windows, el controlador de dominio y los intervalos IP según el punto de distribución:

  - **Sondeo de dominios de Windows**

    Puede habilitar y programar el descubrimiento de dispositivos en los dominios de Windows.

  - **Sondeo del controlador de dominio**

    Puede habilitar y programar el mecanismo de sondeo de red para Active Directory.

    Si utiliza un punto de distribución de Windows, puede seleccionar una de las siguientes opciones:

    - **Sondear el dominio actual de Active Directory**.
    - **Sondear el bosque de dominio de Active Directory**.
    - **Sondear solo los dominios de Active Directory seleccionados**. Si selecciona esta opción, agregue uno o más dominios de Active Directory a la lista.

    Si usa un punto de distribución de Linux con la versión 15 del Agente de red instalada, puede sondear solo los dominios de Active Directory para los cuales especifique la dirección y las credenciales de usuario. El sondeo del dominio de Active Directory actual y el bosque de dominios de Active Directory no está disponible.

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**

- 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 el punto de distribución debe usar 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.

9. 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)** → **Grupos**.
2. En la estructura del grupo de administración, seleccione el grupo de administración para el que desea ver los puntos de distribución asignados.
3. Haga clic en la pestaña **Puntos de distribución**.
4. Añada nuevos puntos de distribución para el grupo de administración utilizando el botón **Asignar** o elimine los puntos de distribución asignados utilizando 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.

Uso de un punto de distribución como servidor push

En Kaspersky Security Center Cloud Console, un punto de distribución puede funcionar como servidor push para dispositivos basados en Windows y Linux administrados por el Agente de red. 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 al mismo grupo de administración, puede habilitar un 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 garantizar la 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 usa un punto de distribución como servidor push, no tiene que enviar paquetes al puerto UDP del Agente de red.

Para usar un punto de distribución como servidor push:

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 punto de distribución que desea usar como servidor push.
4. En la lista de propiedades del punto de distribución seleccionado, vaya a la sección **General** y luego active la opción **Ejecutar servidor push**.

   El campo de entrada del **Puerto del servidor push** pasará a ser disponible.
5. En el campo de entrada **Puerto del servidor push**, especifique el puerto del punto de distribución que los dispositivos cliente usarán para la conexión. De manera predeterminada, se utiliza el puerto 13295.

Para establecer una conexión entre el punto de distribución que actúa como servidor push y un dispositivo administrado, debe agregar manualmente el puerto del servidor push especificado a la lista de exclusión de Firewall de Microsoft Windows.

6. Haga clic en **Aceptar** para salir de la ventana de propiedades del punto de distribución y luego haga clic en **Guardar** para aplicar los cambios.

   Después de activar la opción **Ejecutar servidor push**, la opción **No desconectar del Servidor de administración** se activa automáticamente en el punto de distribución que actúa como servidor push. Esta opción proporciona una conexión temprana entre el Agente de red y el Servidor de administración.

7. Abra la ventana configuración de la directiva del Agente de red.

8. Vaya a **Conectividad** → **Red** y luego active la opción **Usar punto de distribución para forzar la conexión al Servidor de administración**. Cierre el candado para esta opción.

9. Además, en la subsección **Red**, puede desactivar la opción **Usar puerto UDP**. El servidor push configurado proporciona conectividad continua entre un dispositivo administrado y el Servidor de administración en lugar de enviar paquetes a través del puerto UDP.

10. Haga clic en **Aceptar** para salir de la ventana.

El punto de distribución funcionará como servidor push. Ya puede enviar notificaciones push a los dispositivos cliente.

Uso de la opción "No desconectarse del Servidor de administración" para proporcionar conectividad continua entre un dispositivo administrado y el Servidor de administración

Si no utiliza servidores push, Kaspersky Security Center Cloud Console no garantiza la conectividad continua entre los dispositivos administrados y el Servidor de administración. Los Agentes de red en los dispositivos administrados periódicamente establecen conexiones y se sincronizan con el Servidor de administración. El intervalo entre esas sesiones de sincronización se define en una directiva del Agente de red. Si se requiere una sincronización temprana, el Servidor de administración (o un punto de distribución, si está en uso) envía un paquete de red firmado a través de una red IPv4 o IPv6 al puerto UDP del Agente de red. El puerto por defecto es el 15000. Si ninguna conexión a través de UDP es posible entre el Servidor de administración y un dispositivo administrado, la sincronización se ejecutará en la siguiente conexión regular del Agente de red al Servidor de administración dentro del intervalo de sincronización.

Algunas operaciones no se pueden realizar sin una conexión temprana entre el Agente de red y el Servidor de administración, como ejecutar y detener tareas locales, recibir estadísticas para una aplicación administrada o crear un túnel. Para resolver este problema, si no está utilizando servidores push, puede utilizar la opción **No desconectar del Servidor de administración** para garantizar la conectividad continua entre un dispositivo administrado y el Servidor de administración.

Para proporcionar conexión continua entre un dispositivo administrado y el Servidor de administración:

1. Realice una de las siguientes acciones:

   - Si el dispositivo administrado accede al Servidor de administración directamente (es decir, no a través de un punto de distribución):

     a. En el menú principal, vaya a **Dispositivos** → **Dispositivos administrados**.

b. Haga clic en el nombre del dispositivo cuya conectividad continua desea garantizar.

Se abre la ventana de propiedades del dispositivo administrado.

- Si el dispositivo administrado accede al Servidor de administración a través de un punto de distribución que se ejecuta en modo de puerta de enlace, no directamente:

a. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

Se abre la ventana Propiedades del Servidor de administración.

b. En la pestaña **General**, elija la sección **Puntos de distribución**.

c. En la lista de puntos de distribución, haga clic en el nombre del punto de distribución requerido.

Se abre la ventana de propiedades del punto de distribución seleccionado.

2. En la sección **General** de la ventana de propiedades abierta, seleccione la opción **No desconectar del Servidor de administración**.

Hay una conexión continua establecida entre el dispositivo administrado y el Servidor de administración.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

Creación de grupos de administración

Inicialmente, la jerarquía de los grupos de administración contiene un único 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 subgrupos. Para cada grupo de administración, la ventana de propiedades contiene información sobre directivas, tareas y dispositivos relacionados con el grupo.

Para crear un grupo de administración:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. Seleccione la casilla de verificación junto al grupo de administración para el que desea crear un nuevo subgrupo.
3. Haga clic en el botón **Añadir**.
4. Escriba un nombre para el nuevo grupo de administración.
5. Haga clic en el botón **Añadir**.

Aparece un nuevo grupo de administración con el nombre especificado en la jerarquía de los grupos de administración.

La aplicación permite crear una jerarquía de grupos de administración basada en la estructura de Active Directory o en la estructura de la red de dominios. También es posible crear una estructura de grupos a partir de un archivo de texto.

Para crear una estructura de grupos de administración:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. Haga clic en el botón **Importar**.

Se inicia el Asistente de nueva estructura de grupos de administración. Siga las instrucciones del asistente.

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 se selecciona la opción **Aplicar regla permanentemente**, la regla de movimiento se aplica independientemente de la configuración de prioridad. Dichas reglas se aplican de acuerdo con la programación que el Servidor de administración configura automáticamente.

Si los atributos de dispositivo cumplen con las condiciones de varias reglas, el dispositivo se mueve al grupo de destino de la regla con la prioridad más alta (es decir, la que tiene la clasificación más alta en la lista de reglas).

Copiar reglas de movimiento de dispositivos

Puede copiar sus reglas de movimiento de dispositivos si, por ejemplo, desea tener varias reglas de movimiento idénticas para diferentes grupos de administración de destino.

Para copiar una regla de movimiento existente:

1. Realice una de las siguientes acciones:

   - En el menú principal, vaya a **Activos (dispositivos)** → **Reglas de movimiento**.

   - En el menú principal, vaya a **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.
- Información sobre la unidad organizativa (OU) de Active Directory con los dispositivos cliente.
- Información sobre un segmento de nube con los dispositivos cliente.

A continuación, puede encontrar la descripción sobre cómo especificar esta información en una regla de movimiento de dispositivos.

Si especifica varias condiciones en la regla, se usa el operador lógico AND y todas las condiciones se aplican al mismo tiempo. Si no selecciona ninguna opción o deja algunos campos en blanco, dichas condiciones no se aplican.

Pestaña Etiquetas

En esta pestaña, puede configurar una búsqueda del dispositivo según las etiquetas para dispositivos que se añadieron anteriormente a las descripciones de los dispositivos administrados: Para hacerlo, seleccione las etiquetas pertinentes. Además, puede habilitar las siguientes opciones:

- **Aplicar a los dispositivos que no tengan 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 del dispositivo en la red de Windows**

  Nombre de red de Windows (nombre NetBIOS) del dispositivo, o la dirección IPv4 o IPv6.

- **Dominio de Windows**

  Una regla de movimiento de dispositivos se aplica a todos los dispositivos incluidos en el dominio de Windows especificado.

- **Nombre DNS del dispositivo**

  Nombre de dominio DNS del dispositivo cliente que desea mover. Complete este campo si su red incluye un servidor DNS.

  Si la intercalación de la distinción entre mayúsculas y minúsculas está configurada para la base de datos que usa para Kaspersky Security Center Cloud Console, 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.

- **El dispositivo está en el rango IP**

  Si esta opción está activada, puede seleccionar un rango de IP que haya agregado previamente en la sección **Rangos IP**. Los dispositivos relevantes deben estar incluidos en el rango IP seleccionado.

  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 15.3** o **Servidor de administración de Kaspersky Security Center 15.3**.

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 las columnas** ( ) 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 habilitada, se aplica una regla de movimiento de dispositivos a los dispositivos de la unidad organizativa de Active Directory especificados en la lista que hay debajo de la opción.

  Esta opción está deshabilitada de manera predeterminada.

- Incluir unidades organizativas secundarias

  Si habilita esta opción, la selección incluirá los dispositivos de todas las unidades organizativas secundarias de la unidad organizativa de Active Directory especificada.

  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**
- Incluir el dispositivo en el siguiente grupo de seguridad de dominio

  Si esta opción está habilitada, se aplica una regla de movimiento de dispositivos a los dispositivos de la unidad organizativa de Active Directory especificados en la lista que hay debajo de la opción.

  Esta opción está deshabilitada de manera predeterminada.

Pestaña Segmentos de la nube

En esta pestaña, puede especificar que es necesario mover los dispositivos que pertenecen a segmentos de la nube específicos:

- El dispositivo está en un segmento de la nube

  Si selecciona esta opción, una regla de movimiento de dispositivos se aplica a los dispositivos cliente que pertenecen a un segmento de la nube. Puede seleccionar el segmento de nube requerido hasta una subred en la lista que hay debajo de la opción.

  La opción está desactivada de forma predeterminada.

- Incluir objetos secundarios

  Si selecciona esta opción, se aplica una regla de movimiento de dispositivos no solo al segmento de nube seleccionado, sino también a los objetos secundarios de este segmento.

  La opción está desactivada de forma predeterminada.

- **Mover dispositivos desde objetos anidados a subgrupos correspondientes**
- **Crear subgrupos correspondientes a contenedores de dispositivos detectados recientemente**
- **Eliminar subgrupos para los que no se encontró coincidencia en los segmentos de la nube**
- Dispositivo descubierto mediante la API

La lista desplegable le permite operar con el hecho de que el dispositivo pueda detectarse con las herramientas provistas por una API.

- **AWS**. El dispositivo se descubre mediante la API de AWS, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de AWS.
- **Azure**. El dispositivo se descubre mediante la API de Azure, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Azure.
- **Google Cloud.** El dispositivo se descubre utilizando la API de Google, es decir, el dispositivo está en el entorno de Google Cloud.
- **No**. El dispositivo no se puede detectar con la API de AWS, Azure o Google (o bien el dispositivo no se encuentra en el entorno de nube, o bien sí está en el entorno de nube, pero, por algún motivo, no se lo puede detectar con una API).
- **Ningún valor.** Esta condición no se aplica.

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. Elija el grupo de administración al que pertenezcan los dispositivos que desee añadir:
   - Para el grupo raíz, haga lo siguiente:

     En este caso, puede continuar con el siguiente paso.
   - Para un subgrupo:

     Haga clic en el botón **Cambiar alcance** en la parte superior de la página y, luego, en la ventana que se abre, haga clic en el nombre del subgrupo.

     La ruta al grupo elegido se muestra en la parte superior de la página. Si es necesario, puede hacer clic en un enlace con el nombre del grupo de administración para ir al grupo. De manera predeterminada, el último enlace de la ruta está inactivo.
3. Haga clic en el botón **Añadir dispositivos**.

   Se inicia el Asistente para mover dispositivos.
4. 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 los nombres NetBIOS o los nombres DNS de los dispositivos.

    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: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

5. 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.
6. 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)** → **Grupos** → **<nombre del grupo>** → **Dispositivos administrados**.
   - 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.

Configuración de reglas de retención para dispositivos no asignados

Una vez finalizado el sondeo de la red de Windows, los dispositivos descubiertos se colocan en subgrupos del grupo de administración "Dispositivos no asignados". Este grupo de administración se encuentra en **Detección y despliegue** → **Detección** → **Dominios de Windows**. El grupo primario es la carpeta **Dominios de Windows**. Dicha carpeta contiene grupos secundarios que llevan el nombre de los dominios y grupos de trabajo descubiertos durante el sondeo. El grupo primario también puede contener el grupo de administración de dispositivos móviles. Puede configurar las reglas de retención de dispositivos no asignados para el grupo primario y para cada uno de los grupos secundarios. Las reglas de retención no dependen de la configuración del descubrimiento de dispositivos y funcionan incluso si el descubrimiento de dispositivos está deshabilitado.

Las reglas de retención de dispositivos no afectan a los dispositivos que tienen una o más unidades cifradas con cifrado de disco completo. Dichos dispositivos no se eliminan automáticamente, solo puede hacerlo de forma manual. Si necesita eliminar un dispositivo con una unidad cifrada, primero descifre la unidad y luego elimine el dispositivo.

Para configurar las reglas de retención para dispositivos no asignados:

1. En el menú principal, vaya a **Detección y despliegue** → **Detección** → **Dominios de Windows**.
2. Realice una de las siguientes acciones:
   - Para configurar los ajustes del grupo primario, haga clic en el botón **Propiedades**.

     Se abrirá la ventana de propiedades del dominio de Windows.
   - Para configurar los ajustes de un grupo secundario, haga clic en su nombre.

     Se abrirá la ventana de propiedades del grupo secundario.
3. Defina los siguientes parámetros de configuración:
   - **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. De forma predeterminada, esta opción se propaga a los grupos secundarios. El intervalo de tiempo por defecto es de 7 días.

     Esta opción está habilitada de manera predeterminada.
   - **Heredar del grupo primario**

Si esta opción está habilitada, el período de retención de dispositivos en el grupo seleccionado se heredará del grupo primario y no se podrá modificar.

Esta opción solo está disponible para grupos secundarios.

Esta opción está habilitada de manera predeterminada.

- **Forzar herencia en grupos secundarios**

  Los valores de configuración se propagarán a los grupos secundarios. Los ajustes correspondientes estarán bloqueados en las propiedades de esos grupos.

  Esta opción está deshabilitada de manera predeterminada.

4. Haga clic en el botón **Aceptar**.

Se guardarán y aplicarán los cambios.

Configurar la protección de la red

En esta sección, encontrará información sobre la configuración manual de tareas y directivas, sobre los roles de usuario y sobre la creación de una jerarquía de tareas y una estructura de grupos de administración.

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 inadmisible) para su organización. Por este motivo, recomendamos que modifique estas directivas y tareas predeterminadas y que, de ser necesario, cree otras directivas y tareas adicionales para su red.

Requisitos previos

Antes de comenzar, asegúrese de haber completado el escenario de configuración inicial de Kaspersky Security Center Cloud Console, incluido el asistente de inicio rápido.

Cuando el asistente de inicio rápido se está ejecutando, se crean las siguientes directivas y tareas en el grupo de administración **Dispositivos administrados**:

- Directiva de Kaspersky Endpoint Security
- Tarea de grupo para actualizar Kaspersky Endpoint Security
- Directiva del Agente de red
- Encontrar vulnerabilidades y configuraciones de tareas de actualizaciones requeridas (tarea 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. También puede combinar estos dos enfoques.

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
   - Creación de la tarea *Buscar vulnerabilidades y actualizaciones requeridas*

   Si es necesario, cree tareas adicionales para administrar las aplicaciones Kaspersky instaladas en los dispositivos cliente.

3. **Evaluar y limitar el impacto de los eventos en la base de datos**

Se transfiere la información sobre eventos que ocurren durante el funcionamiento de aplicaciones administradas de un dispositivo cliente y se la registra en la base de datos del Servidor de administración. Para reducir la carga 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. Los dispositivos también pueden diferenciarse sobre la base de sus especificaciones de hardware o de su uso en Active Directory.

El enfoque centrado en el usuario permite configurar las aplicaciones de seguridad de maneras diferentes para roles de usuario diferentes. Puede crear una serie de roles de usuario, asignarlos a sus usuarios según las funciones que desempeñen en la empresa y luego crear configuraciones diferentes, que se apliquen a uno u otro dispositivo según el rol asignado al propietario del dispositivo. Imagine, por ejemplo, que una aplicación de Kaspersky debe estar configurada de un modo diferente si se encuentra instalada en el dispositivo de un contador o en el dispositivo de un especialista en RR. HH. Al implementar la administración de la seguridad centrada en el usuario, puede hacer que cada departamento (el de Contabilidad y el de Recursos Humanos) tenga su propio "juego de ajustes" para esa aplicación. El juego de ajustes determina qué valores de configuración pueden ser modificados por los usuarios y cuáles se imponen por la fuerza y solamente pueden ser modificados por el administrador.

El enfoque centrado en el usuario también permite configurar una aplicación de un modo específico para un usuario específico. Esto puede ser útil si hay un empleado con un rol único en la empresa o si se quieren supervisar los problemas de seguridad asociados a los dispositivos de una persona en particular. El rol de este empleado en particular podría determinar si la persona tendrá más o menos derechos para modificar los ajustes de la aplicación. Un administrador de sistemas que tenga a su cargo los dispositivos cliente de una oficina local podría necesitar más derechos que otros usuarios.

El enfoque centrado en el dispositivo y el enfoque centrado en el usuario pueden combinarse. Podría, por ejemplo, configurar una directiva de aplicación específica para cada uno de sus grupos de administración y, luego, podría crear perfiles de directivas que se apliquen a uno o más de los roles de usuario definidos en su empresa. Si hace esto, las directivas y los perfiles se aplicarán en el siguiente orden:

1. Se aplicarán las directivas creadas en el marco del enfoque centrado en el dispositivo.
2. Los perfiles modificarán las directivas siguiendo el orden de prioridad definido para los perfiles de directivas.
3. Los perfiles de directivas vinculados a los roles de usuario modificarán las directivas.

Configuración y propagación de directivas: enfoque centrado en el dispositivo

Esta sección describe el escenario de enfoque centrado en el dispositivo para la configuración centralizada 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.

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.

Proceso

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 Cloud Console crea la directiva predeterminada para Kaspersky Endpoint Security para Windows. Si completó el proceso de configuración utilizando este asistente, no tiene que crear una nueva directiva para esta aplicación. En cambio, puede sencillamente configurar la directiva de Kaspersky Endpoint Security en forma manual.

   Si tiene una estructura jerárquica de varios grupos de administración, los grupos de administración secundarios heredan las directivas del Servidor de administración principal de forma predeterminada. Puede forzar la herencia de los grupos secundarios para prohibir cualquier modificación de los parámetros 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. Las configuraciones desbloqueadas restantes estarán disponibles para modificarse 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.

A través de las condiciones de activación, podrá aplicar perfiles de directivas diferentes a, por ejemplo, los dispositivos que pertenezcan a ciertas unidades o a ciertos grupos de seguridad de Active Directory, a los que tengan configuraciones de hardware específicas o a los que estén marcados con etiquetas específicas. Puede usar las etiquetas para filtrar dispositivos que reúnen criterios específicos. Podría, por ejemplo, crear una etiqueta llamada *Windows*, marcar con ella los dispositivos que utilicen el sistema operativo Windows y especificarla como condición de activación para un perfil de directiva. Ello hará que las aplicaciones de Kaspersky instaladas en dispositivos con Windows queden sujetas a un perfil de directiva específico.

Instrucciones:

- 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**

   Kaspersky Security Center Cloud Console sincroniza automáticamente el Servidor de administración con los dispositivos administrados varias veces por hora. Las directivas nuevas o con cambios y los perfiles de directivas se propagan a los dispositivos administrados durante la sincronización. Puede saltear la sincronización automática y realizar una sincronización manual a través del comando "Forzar sincronización". Una vez que se completa la sincronización, las directivas y los perfiles de directivas se entregan y aplican a las aplicaciones de Kaspersky instaladas.

   Puede verificar si las directivas y los perfiles de directivas se entregaron a un dispositivo. Kaspersky Security Center Cloud Console 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.

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 Cloud Console 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. En cambio, puede sencillamente configurar la directiva de Kaspersky Endpoint Security en forma manual.

Si tiene una estructura jerárquica de varios grupos de administración, los grupos de administración secundarios heredan las directivas del Servidor de administración principal de forma predeterminada. Puede forzar la herencia de los grupos secundarios para prohibir cualquier modificación de los parámetros 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. Las configuraciones desbloqueadas restantes estarán disponibles para modificarse 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**

Kaspersky Security Center Cloud Console sincroniza automáticamente el Servidor de administración con los dispositivos administrados varias veces por hora. Las directivas nuevas o con cambios y los perfiles de directivas se propagan a los dispositivos administrados durante la sincronización. Puede saltear la sincronización automática y realizar una sincronización manual a través del comando "Forzar sincronización". Una vez que se completa la sincronización, las directivas y los perfiles de directivas se entregan y aplican a las aplicaciones de Kaspersky instaladas.

Puede verificar si las directivas y los perfiles de directivas se entregaron a un dispositivo. Kaspersky Security Center Cloud Console especifica la fecha y la hora de entrega en las propiedades del dispositivo.

Instrucciones: Sincronización forzada

Resultados

Al concluir este proceso, las aplicaciones de Kaspersky tendrán la configuración especificada y propagada a través de la jerarquía de directivas y perfiles de directivas.

Cuando necesite sumar un nuevo usuario, cree una cuenta nueva para esa persona y asígnele los dispositivos que usará y uno de los roles de usuario que haya creado. Las directivas y los perfiles de directivas que haya configurado para las aplicaciones se aplicarán automáticamente a los dispositivos del nuevo usuario.

Ajustes de la directiva del Agente de red

Para configurar la directiva del Agente de red:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva del Agente de red.

   Se abre la ventana de propiedades de la directiva del Agente de red.

Consulte la tabla comparativa que detalla cómo se aplican los siguientes ajustes según el tipo de sistema operador que se use.

Pestaña General

En esta pestaña puede modificar el estado de la directiva y especificar la herencia de la configuración de la directiva:

- En el bloque **Estado de la directiva**, puede seleccionar uno de los modos de directiva:
  - **Activa**
  - **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 principal**

Si habilita esta opción, la directiva heredará los valores de configuración definidos en la directiva del grupo de nivel superior. Estos valores, en consecuencia, estarán bloqueados.

Esta opción está 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.

Pestaña Configuración de eventos

Esta ficha le permite configurar el registro de eventos y la notificación de eventos. Los eventos se organizan por nivel de importancia en las siguientes secciones de la pestaña **Configuración de eventos**:

- **Fallo operativo**
- **Advertencia**
- **Información**

Cada sección contiene una lista con los distintos tipos de eventos y, junto a ellos, la cantidad de días por los que cada evento se deja almacenado, por defecto, en el Servidor de administración. Si hace clic en el botón **Propiedades**, puede especificar la configuración del registro de eventos y las notificaciones sobre los eventos seleccionados en la lista. De forma predeterminada, la configuración de notificación común especificada para todo el Servidor de administración se usa para todos los tipos de eventos. Si lo necesita, puede modificar ajustes puntuales para los tipos de eventos que requieran cambios.

Pestaña 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 esta opción está activada, los dispositivos cliente recibirán actualizaciones solo a través de los puntos de distribución, y no directamente desde los servidores de actualización.

  Si esta opción está desactivada, los dispositivos cliente podrán recibir actualizaciones desde varias fuentes: directamente desde servidores de actualización y desde una carpeta local o carpeta de red.

  Esta opción está deshabilitada de manera predeterminada.

- **Tamaño máximo de la cola del evento, en MB**

- **La aplicación podrá obtener información adicional sobre la directiva en el dispositivo**

  La aplicación de seguridad de un dispositivo administrado (por ejemplo, Kaspersky Endpoint Security para Windows) recibe, del Agente de red instalado en el mismo dispositivo, información sobre la directiva que para ella se ha aplicado. Si lo desea, puede ver esta información en la interfaz de la aplicación de seguridad.

  El Agente de red le brinda los siguientes datos a la aplicación:

  - Hora en que la directiva se entregó en el dispositivo administrado.
  - Nombre de la directiva activa que se encontraba vigente cuando la directiva se entregó en el dispositivo administrado.
  - Nombre de la directiva fuera de la oficina que se encontraba vigente cuando la directiva se entregó en el dispositivo administrado (no disponible en el Agente de red para Linux).
  - Nombre y ruta completa al grupo de administración en el que se encontraba el dispositivo administrado cuando la directiva se entregó en el dispositivo administrado.
  - Lista de perfiles de directivas activas que se encontraban vigentes cuando la directiva se entregó en el dispositivo administrado, con sus nombres y prioridades.

  Puede utilizar esta información para solucionar problemas o verificar que la directiva aplicada al dispositivo sea la esperada. Esta opción está deshabilitada de 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.

  Note que la utilidad klmover se usa solo para mover dispositivos administrados bajo la administración de un Servidor de administración virtual.

  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**
- Incluir información sobre parches

  Se enviará información al Servidor de administración sobre los parches de las aplicaciones instaladas en los dispositivos clientes. Si habilita esta opción, podría aumentar la carga del Servidor de administración y del sistema de administración de bases de datos (DBMS). También podría aumentar el volumen de la base de datos.

  Esta opción está habilitada de manera predeterminada. Está disponible solo para Windows.

- Detalles de las actualizaciones de Windows Update

  Si esta opción está habilitada, se enviará información al Servidor de administración sobre las actualizaciones de Microsoft Windows Update que deban instalarse en los dispositivos cliente.

  Aunque deshabilite esta opción, ocasionalmente encontrará actualizaciones en la sección **Actualizaciones disponibles** de las propiedades de un dispositivo. Esto podría suceder, por ejemplo, cuando los dispositivos de la organización tengan vulnerabilidades que puedan repararse con esas actualizaciones.

  Esta opción está habilitada de manera predeterminada. Está disponible solo para Windows.

  La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

- Detalles de vulnerabilidades de software y actualizaciones correspondientes

  Si esta opción está habilitada, se enviará información al Servidor de administración sobre las vulnerabilidades que se detecten en las aplicaciones de terceros instaladas en los dispositivos administrados (incluidas las aplicaciones de Microsoft) y sobre las actualizaciones disponibles para reparar vulnerabilidades en aplicaciones de terceros (excluidas, en este caso, las aplicaciones de Microsoft).

  Si habilita la opción **Detalles de vulnerabilidades de software y actualizaciones correspondientes**, aumentarán la carga en la red, la carga en el disco del Servidor de administración y el uso de recursos del Agente de red.

  Esta opción está habilitada de manera predeterminada. Está disponible solo para Windows.

  Para administrar las actualizaciones de software de Microsoft, use la opción **Detalles de las actualizaciones de Windows Update**.

- **Detalles de registro de hardware**

Vulnerabilidades y actualizaciones de software

En la sección **Vulnerabilidades y actualizaciones de software**, puede configurar la búsqueda de actualizaciones de Windows, así como activar el análisis de archivos ejecutables en busca de vulnerabilidades. La configuración en la sección **Vulnerabilidades y actualizaciones de software** está disponible solo en dispositivos que ejecutan Windows:

- Utilice el grupo de opciones **Modo de búsqueda de Windows Update** para seleccionar el modo de búsqueda de actualizaciones:
  - Activo

Si selecciona esta opción, el Servidor de administración (asistido por el Agente de red) hará que el Agente de Windows Update del dispositivo cliente realice una solicitud al origen de actualizaciones (los servidores de Windows Update o WSUS). Tras ello, el Agente de red transmitirá al Servidor de administración la información que reciba del Agente de Windows Update.

Esta opción solo tiene efecto si la tarea *Buscar vulnerabilidades y actualizaciones requeridas* tiene habilitada la opción **Conectar al servidor de actualizaciones para actualizar los datos**.

Esta opción está seleccionada de manera predeterminada.

- **Pasivo**

  Si selecciona esta opción, el Agente de red se comunicará periódicamente con el Servidor de administración para enviarle información sobre las actualizaciones obtenidas durante la última sincronización entre el Agente de Windows Update y el origen de actualizaciones. Si el Agente de Windows Update no se sincroniza con un origen de actualizaciones, la información sobre actualizaciones del Servidor de administración se vuelve obsoleta.

  Seleccione esta opción si desea obtener actualizaciones de la caché del origen de actualizaciones.

- **Desactivado**

  Si selecciona esta opción, el Servidor de administración no solicitará información sobre las actualizaciones.

  Seleccione esta opción si, por ejemplo, desea probar primero las actualizaciones en su dispositivo local.

- **Analizar los archivos ejecutables para buscar vulnerabilidades al iniciarlos**

  Si habilita esta opción, cuando se inicie un archivo ejecutable, se lo analizará en busca de vulnerabilidades.

  Esta opción está deshabilitada de manera predeterminada.

Administración de reinicios

En la sección **Administración de reinicios**, puede indicar qué acción se llevará a cabo cuando se necesite reiniciar el sistema operativo de un dispositivo administrado para que una aplicación pueda instalarse, desinstalarse o utilizarse correctamente.

- **No reiniciar el sistema operativo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o 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.

Escritorio compartido de Windows

En la sección **Escritorio compartido de Windows**, puede habilitar y configurar la auditoría de las acciones del administrador realizadas en un dispositivo remoto cuando se comparte el acceso al escritorio. Los ajustes en el **Escritorio compartido de Windows** están disponibles solo en dispositivos que ejecutan Windows:

- **Activar auditoría**

Habilite esta opción si desea auditar las operaciones que el administrador realice en el dispositivo remoto. Los registros de las acciones del administrador en el dispositivo remoto se computan:

- En el registro de eventos del dispositivo remoto
- en un archivo con la extensión syslog ubicado en la carpeta de instalación del Agente de red del dispositivo remoto
- En la base de datos de eventos de Kaspersky Security Center Cloud Console

La auditoría de las acciones del administrador está disponible cuando se cumplen las siguientes condiciones:

- La licencia de Administración de vulnerabilidades y parches está en uso
- El administrador tiene permiso para ejecutar el acceso compartido al escritorio del dispositivo remoto

Si no necesita auditar las operaciones del administrador en el dispositivo remoto, no habilite esta opción.

Esta opción está deshabilitada de manera predeterminada.

- **Máscaras de archivos cuya lectura se debe supervisar**

  La lista contiene máscaras de archivos. Cuando la auditoría está habilitada, la aplicación monitorea los archivos de lectura del administrador que coinciden con las máscaras y guarda información sobre los archivos leídos. La lista está disponible si se ha marcado la casilla **Habilitar auditoría**. Puede editar máscaras de archivos y agregar máscaras nuevas a la lista. Cada máscara de archivo nueva se debe especificar en la lista en una línea nueva.

  De forma predeterminada, están especificadas las siguientes máscaras de archivos:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Máscaras de archivos cuya modificación se debe supervisar**

  La lista contiene las máscaras de archivos en el dispositivo remoto. Cuando la auditoría está habilitada, la aplicación monitorea los cambios realizados por el administrador en los archivos que coinciden con las máscaras y guarda información sobre esas modificaciones. La lista está disponible si se ha marcado la casilla **Habilitar auditoría**. Puede editar máscaras de archivos y agregar máscaras nuevas a la lista. Cada máscara de archivo nueva se debe especificar en la lista en una línea nueva.

  De forma predeterminada, están especificadas las siguientes máscaras de archivos:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Administrar parches y actualizaciones

En la sección **Administrar parches y actualizaciones**, puede configurar la descarga y distribución de actualizaciones, así como la instalación de parches, en los dispositivos administrados: activar o desactivar la opción **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir**.

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 configuración **Conexión al Servidor de administración**, puede especificar la siguiente configuración:

  - 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 activa esta opción, se añaden los puertos 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 la puerta de enlace de conexión de un 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 el Agente de red se conecte al Servidor de administración 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. El puerto UDP predeterminado de conexión al Servidor de administración es 15000.

- Número de puerto UDP

  En este campo, puede indicar el número del puerto UDP. El número de puerto predeterminado es el 15000.

  El sistema decimal se usa para los registros.

  En dispositivos cliente con Windows XP Service Pack 2, el puerto UDP 15000 estará bloqueado por el firewall integrado. Deberá abrir el puerto manualmente.

- Usar el punto de distribución para forzar una conexión con el Servidor de administración

Seleccione esta opción si seleccionó la opción **Ejecutar servidor push** en la ventana de configuración del punto de distribución. De lo contrario, el punto de distribución no funcionará como un servidor push.

En la subsección **Perfiles de conexión** no se pueden añadir nuevos elementos a la lista **Perfiles de conexión al Servidor de administración**, así que el botón **Añadir** está inactivo. Los perfiles de conexión preestablecidos tampoco se pueden modificar.

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**
- **Conectarse en los intervalos de tiempo especificados**

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. Los ajustes de sondeo solo están disponibles en dispositivos con Windows. Puede utilizar las siguientes opciones para habilitar el sondeo y definir una frecuencia de sondeo:

- Red de Windows

  Si esta opción está activada, el punto de distribución sondea automáticamente la red según la planificación que se configura al hacer clic en los enlaces **Programar un sondeo rápido** y **Programar un sondeo completo**.

  Si esta opción está desactivada, el Servidor de administración no sondea la red.

  Esta opción está habilitada de manera predeterminada.

- Rangos IP

  Si esta opción está activada, el punto de distribución sondea automáticamente los rangos de IP según la planificación que se configura al hacer clic en el enlace **Programar sondeo**.

  Si esta opción está desactivada, el punto de distribución no sondea rangos de IP.

  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

  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**
- **Contraseña**

Proxy de KSN (puntos de distribución)

En la sección **Proxy de KSN (puntos de distribución)**, puede configurar la aplicación para que utilice el punto de distribución para reenviar las solicitudes 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.

Esta característica no es compatible con dispositivos de puntos de distribución que ejecuten Linux o macOS.

El punto de distribución enviará a Kaspersky las estadísticas de KSN que se enumeran en la declaración de Kaspersky Security Network. De forma predeterminada, la declaración de KSN se encuentra en %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

Esta opción está deshabilitada de manera predeterminada. Esta opción solo se activa si la opción **Acepto usar Kaspersky Security Network** está activada 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.

- **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 el Agente de red se conecte al Servidor de administración 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. El puerto UDP predeterminado de conexión al Servidor de administración es 15000.

Comparación de la configuración de la directiva del Agente de red por sistemas operativos

La siguiente tabla muestra qué configuración de directiva del Agente de red puede usar para configurar el Agente de red con un sistema operativo específico.

Configuración de la directiva del Agente de red: comparación por sistemas operativos

Sección de la directiva	Windows	macOS	Linux
General	✓	✓	✓
Configuración de eventos	✓	✓	✓
Configuración	✓	✓ Excepto la casilla **Utilizar contraseña de desinstalación**	✓ Excepto la casilla **Utilizar contraseña de desinstalación**
Repositorios	✓	✓ La opción **Detalles de registro de hardware** está disponible.	✓ Las siguientes opciones están disponibles: • **Detalles de las aplicaciones instaladas** • **Detalles de registro de hardware**

Vulnerabilidades y actualizaciones de software	✓	—	—
Administración de reinicios	✓	—	—
Escritorio compartido de Windows	✓	—	—
Administrar parches y actualizaciones	✓	—	—
Conectividad → Red	✓	✓ Excepto la casilla **Abrir puertos del Agente de red en el Firewall de Microsoft Windows**.	✓ Excepto la casilla **Abrir puertos del Agente de red en el Firewall de Microsoft Windows**.
Conectividad → Programación de conexiones	✓	✓	✓
Sondeo de la red realizado por los puntos de distribución	✓ Las siguientes opciones están disponibles: • **Red de Windows** • **Rangos IP** • **Controladores de dominio** (Microsoft Active Directory)	—	✓ Las siguientes opciones están disponibles: • **Rangos IP** • **Controladores de dominio** (Microsoft Active Directory, Samba como Active Directory)
Configuración de red para puntos de distribución	✓	✓	✓
Proxy de KSN (puntos de distribución)	✓	—	✓

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 tiene 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.

Puede configurar el funcionamiento de Kaspersky Security Network en la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows, en la sección **Configuración de la aplicación → Protección frente a amenazas avanzadas**.

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 frente a amenazas avanzadas** → **Kaspersky Security Network**.
4. Asegúrese de que la opción **Utilizar Servidor de administración como servidor proxy de KSN** esté activada. Esta función ayuda a redistribuir y optimizar el tráfico de la red.

   Si utiliza Managed Detection and Response, debe activar la opción **Kaspersky Security Network** para el punto de distribución y activar el modo de KSN extendido.
5. Active el uso de servidores KSN si el servicio del proxy de KSN no está disponible. Para ello, active la opción **Utilizar servidores de Kaspersky Security Network si el servidor proxy de KSN no esté 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 de seguridad, los firewalls o los filtros no protegen los dispositivos de dicha red.
- **Red local**. El acceso a archivos e impresoras está restringido para dispositivos en esta red.
- **Red de confianza**. Los dispositivos en dicha red están protegidos contra ataques y accesos no autorizados a archivos y datos.

Si ha configurado una red personalizada, asegúrese de que el Firewall la proteja. Para ello, consulte la lista de redes en las propiedades de la directiva de Kaspersky Endpoint Security 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 frente a amenazas básicas** → **Firewall**.

4. En **Redes disponibles**, haga clic en el enlace **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.

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 activa en la directiva de nivel superior, desmarque la casilla **Acerca de 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 Cloud Console (docenas de gigabytes).

La base de datos del Servidor de administración ya no contendrá información sobre los módulos de software instalados.

Configurar el registro de eventos de directiva importantes en la base de datos del Servidor de administración

Para evitar el desbordamiento de la base de datos del Servidor de administración, recomendamos que solo guarde eventos importantes en la base de datos. Para los eventos que considere poco importantes, puede reducir o desactivar el período de almacenamiento.

Para ajustar la configuración del almacenamiento de eventos:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en el nombre de la directiva pertinente.

   Se abrirá la ventana de propiedades de la directiva seleccionada.

3. Vaya a la pestaña **Configuración de eventos** y haga clic en el nombre del tipo de evento para el que desea configurar el registro en la base de datos.

4. En el panel derecho que se abre, realice una de las siguientes acciones:

   - Si desea cambiar el período de almacenamiento para el tipo de evento, asegúrese de que la opción **Almacenar en la base de datos del Servidor de administración durante (días)** está activada y, a continuación, introduzca la cantidad de días que se debe almacenar el tipo de evento.

   - Si no desea almacenar el tipo de evento en la base de datos del Servidor de administración, desactive la opción **Almacenar en la base de datos del Servidor de administración durante (días)**.

5. Haga clic en **Aceptar** y, una vez que se cierre el panel derecho, haga clic en el botón **Guardar**.

Se cierra la ventana de propiedades de la directiva y se aplica la configuración que seleccionó.

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 la tarea** está seleccionada.

Tareas

Esta sección describe tareas utilizadas por Kaspersky Security Center Cloud Console.

Acerca de las tareas

Kaspersky Security Center Cloud Console administra las aplicaciones de seguridad de Kaspersky instaladas en dispositivos mediante la creación y ejecución de tareas. Las *tareas* son necesarias para instalar, iniciar y detener aplicaciones, analizar archivos, actualizar bases de datos y módulos de software, y realizar otras acciones en las aplicaciones. Una tarea se puede ejecutar en el Servidor de administración o en un dispositivo.

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 que usa herramientas de administración, 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.

- *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 varias 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 la ejecución de las tareas se guardan en el registro de eventos del sistema operativo de cada dispositivo y en la base de datos del servidor de administración.

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

Acerca del alcance de las tareas

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

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

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

- Especificar dispositivos puntuales manualmente.

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

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

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

- Especificar una selección de dispositivos.

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

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

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

Crear una tarea

Puede crear una tarea en la lista de tareas. O bien, puede elegir dispositivos en la lista **Dispositivos administrados** y crear una nueva tarea asignada a los dispositivos elegidos.

Para crear una tarea en la lista de tareas:

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:

En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

Se muestra la lista de dispositivos administrados.

1. 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.
2. Haga clic en el botón **Ejecutar tarea** y, luego, seleccione **Crear 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.
3. Haga clic en el botón **Finalizar**.

La tarea se crea para los dispositivos seleccionados.

Ver la lista de tareas

Puede ver la lista de tareas que se crean en Kaspersky Security Center Cloud Console.

Para ver la lista de tareas:

En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.

Se muestra la lista de tareas. Las tareas se agrupan en torno a los nombres de las aplicaciones con las que están relacionadas. Por ejemplo, la tarea *Desinstalar aplicación en remoto* está relacionada con el Servidor de administración y *Buscar vulnerabilidades y actualizaciones requeridas* se refiere al Agente de red.

Para ver las propiedades de una tarea:

Haga clic en el nombre de la tarea.

Aparece la ventana de propiedades de la tarea. En ella encontrará una serie de pestañas con nombre. La pestaña llamada **General** contiene la propiedad **Tipo de tarea**, por ejemplo, y si ingresa a la pestaña **Programación**, encontrará la programación de la tarea.

Iniciar una tarea manualmente

La aplicación inicia las tareas siguiendo la programación configurada en las propiedades de cada tarea. Puede iniciar una tarea en cualquier momento desde la lista de tareas. O bien, puede elegir dispositivos en la lista **Dispositivos administrados** e iniciar una tarea existente para ellos.

Para iniciar una tarea manualmente:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. En la lista de tareas, 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**.

Iniciar una tarea para los dispositivos seleccionados

Puede seleccionar uno o más dispositivos cliente en la lista de dispositivos y, luego, iniciar una tarea creada previamente para ellos. Esto le permite ejecutar tareas creadas anteriormente para un conjunto específico de dispositivos.

Esto cambia los dispositivos a los que se asignó la tarea a la lista de dispositivos que selecciona cuando ejecuta la tarea.

Para iniciar una tarea para los dispositivos seleccionados:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**. Se muestra la lista de dispositivos administrados.

   En la lista de dispositivos administrados, marque las casillas de verificación de los dispositivos para ejecutar la tarea para ellos. Puede utilizar las funciones de búsqueda y filtrado para encontrar los dispositivos que está buscando.
2. Haga clic en el botón **Ejecutar tarea** y, luego, seleccione **Aplicar tarea existente**.

Se muestra la lista de las tareas existentes.

3. Los dispositivos seleccionados se muestran arriba de la lista de tareas. Si es necesario, puede eliminar un dispositivo de esta lista. Puede eliminar todos los dispositivos menos uno.

4. Seleccione la tarea deseada en la lista. Puede usar el cuadro de búsqueda arriba de la lista para buscar la tarea deseada por nombre. Solo se puede seleccionar una tarea.

5. Haga clic en **Guardar e iniciar tarea**.

La tarea seleccionada se inicia inmediatamente para los dispositivos seleccionados. La configuración de inicio programada en la tarea no se cambia.

Configuración y propiedades generales de las 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.

- Dispositivos a los que se asignará la tarea:
  - **Asignar tarea a un grupo de administración**

    La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

    Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

    Si se asigna una tarea a un grupo de administración, la pestaña **Seguridad** no se muestra en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

  - **Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista**

La tarea se asignará a ciertos dispositivos específicos. Puede especificar los dispositivos mediante uno de los siguientes métodos:

- Especifique la dirección IP, el nombre NetBIOS o el nombre DNS del dispositivo.
- Especifique el rango IP.

  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.
- Seleccione los dispositivos detectados por el Servidor de administración, incluidos los 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.

- **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.

- 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.

- Ajustes de reinicio del sistema operativo:
  - **No reiniciar**

    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)**

  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.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está 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.

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.

- Programación de la tarea:
  - **Iniciar tarea (ajuste):**
    - **Manualmente**

      La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

      Esta opción está seleccionada de manera predeterminada.

    - **Una vez**

      La tarea se ejecuta una vez, en la fecha y hora especificadas (de manera predeterminada, el día en que se ha creado la tarea).

    - **Inmediatamente**

      La tarea se ejecuta inmediatamente después de guardar su configuración.

    - **Cada N minutos**

      La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

      De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

    - **Cada N horas**

La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

De manera predeterminada, la tarea se ejecutará cada 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.

- **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.

  De manera predeterminada, no se selecciona ningún día del mes. La hora de inicio predeterminada es a las 18:00.

- **Cuando se descargan nuevas actualizaciones en el repositorio**

  Cuando se descargan actualizaciones nuevas en los repositorios de puntos de distribución, Kaspersky Security Center Cloud Console ejecuta todas las tareas que tienen esta programación. El Agente de red verifica la disponibilidad de actualizaciones durante la sincronización periódica entre el dispositivo administrado y el Servidor de administración (el latido).

  Por ejemplo, quizá quiera utilizar esta programación para la tarea de actualización relacionada con una aplicación de seguridad, como Kaspersky Endpoint Security.

  Si el Agente de red en un dispositivo administrado no detecta actualizaciones nuevas durante 25 horas o más, entonces Kaspersky Security Center Cloud Console ejecuta en este dispositivo todas las tareas que tienen esta programación. Estas tareas se ejecutan cada hora hasta que se detecten actualizaciones nuevas. Kaspersky Security Center Cloud Console también ejecuta estas tareas cada hora si no hay una conexión entre el dispositivo administrado y el punto de distribución que descarga actualizaciones en el repositorio.

- **Al detectar un brote de virus**

La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

- Antivirus para estaciones de trabajo y servidores de archivos
- Antivirus para defensa del perímetro
- Antivirus para sistemas de correo

Por defecto, están seleccionados todos los tipos de aplicaciones.

En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completar otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. Este parámetro solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Se completó correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Introduzca el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el icono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el icono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

La configuración de programación puede **depender de la zona horaria local del sistema operativo del dispositivo**.

Correlación entre la zona horaria local del sistema operativo del dispositivo y la hora de inicio de la tarea

Programación de tareas	Se utiliza la hora local
Una vez	No
Cada N minutos	No
Cada N horas	No
Cada N días	Sí
Por días de la semana	Sí
Mensualmente	Sí
Cada mes, en días concretos de las semanas seleccionadas	Sí
Cuando se descargan nuevas actualizaciones en el repositorio	Otro disparador para ejecutar la tarea (corresponde al nombre del programa)
Al detectar un brote de virus	Otro disparador para ejecutar la tarea (corresponde al nombre del programa)
Al completar otra tarea	Otro disparador para ejecutar la tarea (corresponde al nombre del programa)
Inmediatamente	Otro disparador para ejecutar la tarea (corresponde al nombre del programa)
Manualmente	Otro disparador para ejecutar la tarea (corresponde al nombre del programa)

- **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 las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manualmente**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de manera predeterminada.

- **Usar el retraso aleatorio automáticamente para el inicio de la tarea**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- Usar el retraso aleatorio automáticamente para el inicio de la tarea con un intervalo de

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está deshabilitada de manera predeterminada. El intervalo de tiempo predeterminado es de un minuto.

- Encender dispositivos mediante la función Wake-on-LAN antes de iniciar la tarea

  El sistema operativo del dispositivo se iniciará a la hora especificada antes de que se ejecute la tarea. El período de tiempo predeterminado es de cinco minutos.

  Habilite esta opción si desea que la tarea se ejecute en todos los dispositivos cliente que formen parte del alcance de la tarea, incluidos aquellos que se encuentren apagados cuando la tarea esté próxima a comenzar.

  Si desea que el dispositivo se apague automáticamente una vez completada la tarea, desactive 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

  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.

- Notificaciones:

  - Bloque **Almacenar el historial de la tarea**:

    - **Guardar todos los eventos**
    - **Guardar eventos sobre el progreso de la tarea**
    - **Guardar solo los resultados de ejecución 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 almacenarán localmente en el registro de eventos de Windows de cada dispositivo cliente.

  Esta opción está deshabilitada de manera predeterminada.

- **Solo notificar errores**
- **Notificar por correo electrónico**

- Ajustes del alcance de la tarea
- Exclusiones de la cobertura

  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 revisión**

Exportar una tarea

Kaspersky Security Center Cloud Console le permite guardar una tarea y sus ajustes 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 Cloud Console 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.

     Si se asigna una tarea a un grupo de administración, la pestaña **Seguridad** no se muestra en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

   - **Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista**

     Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

     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)**.

Ver resultados de la ejecución de tareas almacenados en el Servidor de administración

Kaspersky Security Center Cloud Console le permite ver los resultados de las tareas de grupo, las tareas asignadas a dispositivos específicos y las tareas del Servidor de administración.

Para ver los resultados de la tarea:

1. En la ventana de propiedades de la tarea, seleccione la sección **General**.
2. Haga clic en el enlace **Resultados** para abrir la ventana **Resultados de tarea**.

Administración de dispositivos cliente

Kaspersky Security Center Cloud Console le permite administrar dispositivos cliente:

- Vea la configuración y los estados de los dispositivos administrados, incluidos los clústeres y las matrices de servidores.
- Configure sus puntos de distribución.
- Administre las tareas.

Puede usar grupos de administración para combinar dispositivos cliente en un conjunto que se puede administrar como una sola unidad. Un dispositivo cliente se puede incluir en un solo grupo de administración. Los dispositivos se pueden asignar a un grupo automáticamente sobre la base de las **Condiciones de reglas:**

- Crear reglas de movimiento de dispositivos.
- Copiar reglas de movimiento de dispositivos.
- Condiciones para una regla de movimiento de dispositivos.

Puede usar selecciones de dispositivos para filtrar dispositivos sobre la base de una condición. También puede etiquetar dispositivos para crear selecciones, para buscar dispositivos y para distribuir dispositivos entre grupos de administración.

Configuración de un dispositivo administrado

Para ver la configuración de un dispositivo administrado:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo de su interés.

Se muestra la ventana de propiedades del dispositivo seleccionado.

Las siguientes pestañas se muestran en la parte superior de la ventana de propiedades y representan los principales grupos de ajustes:

- General

Esta pestaña incluye las siguientes secciones:

- La sección **General** muestra información general sobre el dispositivo cliente. La información se basa en los datos recibidos durante la última sincronización del dispositivo cliente con el Servidor de administración.

  - **Nombre**

    En este campo, puede ver y modificar el nombre asignado al dispositivo cliente en el grupo de administración.

  - **Descripción**

    En este campo, puede ingresar una descripción adicional para el dispositivo cliente.

  - **Estado del dispositivo**

    Estado del dispositivo cliente, asignado sobre la base de los criterios definidos por el administrador para el estado de protección antivirus del dispositivo y la actividad del dispositivo en la red.

  - **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 Cloud Console.

- **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.

- **Sesiones**

  Esta sección contiene un contenedor con información sobre los usuarios actualmente conectados al dispositivo. La tabla muestra los siguientes datos en las columnas correspondientes:

  - Nombre de usuario
  - Nombre de la cuenta de SAM
  - Nombre principal del usuario
  - Dirección de correo electrónico

  Para mostrar correctamente la información sobre las sesiones de los usuarios del dominio, debe utilizar el sondeo del controlador de dominio.

- La sección de **Red** muestra la siguiente información sobre las propiedades de red del dispositivo cliente:

  - **Dirección IP**

    Dirección IP del dispositivo.

  - **Dominio de Windows**

    Dominio o grupo de trabajo de Windows en el que está incluido el dispositivo.

  - **Nombre DNS**

    Nombre del dominio DNS del dispositivo cliente.

  - **Nombre NetBIOS**

Nombre de la red de Windows del dispositivo cliente.

- **Dirección IPv6**

- La sección **Sistema** proporciona información sobre el sistema operativo instalado en el dispositivo cliente:
  - **Sistema operativo**
  - **Arquitectura de CPU**
  - **Proveedor del sistema operativo**
  - **Carpeta del sistema operativo**
  - **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.

  - **Compilación del sistema operativo**
- 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.

- La sección **Estado del dispositivo definido por la aplicación** proporciona información sobre el estado del dispositivo definido por la aplicación administrada instalada en el dispositivo. El estado de este dispositivo puede ser diferente al definido por Kaspersky Security Center Cloud Console.

- Aplicaciones

  Esta pestaña enumera todas las aplicaciones de Kaspersky instaladas en el dispositivo cliente. Contiene los botones **Iniciar** y **Detener** que le permiten iniciar y detener la aplicación de Kaspersky seleccionada (pero no el Agente de red). Puede usar estos botones si el puerto 15000 UDP está disponible en el dispositivo administrado para recibir notificaciones push del Servidor de administración. Si el dispositivo administrado no está disponible para notificaciones push, pero el modo de conexión continua al Servidor de administración está activado (la opción **No desconectar del Servidor de administración** en la sección **General** está activada), los botones **Iniciar** y **Detener** también están disponibles. De lo contrario, cuando intenta iniciar o detener la aplicación, se muestra un mensaje de error. También puede hacer clic en el nombre de una aplicación para ver información general sobre la aplicación, los ajustes de configuración de la misma y una lista de los eventos ocurridos en el dispositivo.

- Perfiles de directiva y directivas activas

  Esta pestaña enumera las directivas y los perfiles de directivas que están asignados al dispositivo administrado en un momento dado.

- Tareas

La pestaña **Tareas** permite administrar las tareas del dispositivo cliente. Utilice esta sección para crear tareas nuevas, ver la lista de tareas existentes, ver los resultados de ejecución de las tareas e iniciar, detener, eliminar y reconfigurar las tareas existentes. La lista de tareas mostrada se basa en los datos recibidos durante la última sesión de sincronización entre el cliente y el Servidor de administración. El Servidor de administración solicita detalles sobre el estado de las tareas al dispositivo cliente. Si el puerto 15000 UDP está disponible en el dispositivo administrado para recibir notificaciones push del Servidor de administración, se muestra el estado de la tarea y se activan los botones para administrar la tarea. Si el dispositivo administrado no está disponible para notificaciones push, pero el modo de conexión continua al Servidor de administración está activado (la opción **No desconectar del Servidor de administración** en la sección **General** está activada), las acciones con tareas también están disponibles.

Si no se establece una conexión, no se muestra el estado y los botones quedan desactivados.

- **Eventos**

  La pestaña **Eventos** muestra los eventos registrados en el Servidor de administración para el dispositivo cliente seleccionado.

- **Problemas de seguridad**

  En la pestaña **Problemas de seguridad**, puede ver, crear y editar problemas de seguridad para el dispositivo cliente. Los problemas de seguridad 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.

  Si el Agente de red está instalado en un dispositivo que ejecuta Windows, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo:

  - RAM
  - Dispositivos de almacenamiento masivo
  - Placa madre
  - CPU
  - Adaptadores de red
  - Monitores
  - Adaptador de vídeo
  - Tarjeta de sonido

  Si el Agente de red está instalado en un dispositivo que ejecuta Linux o macOS, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo, si el sistema operativo proporciona esta información:

- Volumen total de la RAM
- Volumen total de los dispositivos de almacenamiento masivo
- Placa madre
- CPU
- Adaptadores de red

- **Actualizaciones disponibles**. Esta sección muestra las actualizaciones de software que se han encontrado en el dispositivo, pero que aún no se han instalado.

- **Vulnerabilidades de software**. Esta sección muestra información sobre las vulnerabilidades de las aplicaciones de terceros instaladas en los dispositivos cliente.

  Para guardar las vulnerabilidades en un archivo, seleccione las casillas junto a las vulnerabilidades que desea guardar, y luego haga clic en el botón **Exportar a CSV** o en el botón **Exportar a TXT**.

  La sección contiene los siguientes ajustes:

  - **Mostrar solo las vulnerabilidades que se pueden reparar**

    Si habilita esta opción, la sección mostrará las vulnerabilidades que se puedan reparar con un parche.

    Si deshabilita esta opción, la sección mostrará tanto las vulnerabilidades que se puedan reparar con un parche como las vulnerabilidades para las que no exista parche publicado.

    Esta opción está habilitada de manera predeterminada.

  - **Propiedades de vulnerabilidad**

    Haga clic en el nombre de una vulnerabilidad de software de la lista para ver las propiedades de la vulnerabilidad de software seleccionada en una ventana aparte. En la ventana, puede hacer lo siguiente:

    - Omita la vulnerabilidad de software en este dispositivo administrado (en la Consola de administración o en Kaspersky Security Center Cloud Console).
    - Ver la lista de reparaciones recomendadas para la vulnerabilidad.
    - Especifique manualmente las actualizaciones de software para corregir la vulnerabilidad (en la Consola de administración o en Kaspersky Security Center Cloud Console).
    - Ver las instancias de la vulnerabilidad.
    - Ver la lista de tareas existentes que permiten reparar la vulnerabilidad y crear tareas de reparación nuevas.

- **Diagnósticos remotos**. En esta sección, puede realizar un diagnóstico remoto de dispositivos cliente.

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 Cloud Console 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 definidas por el usuario* adicionales.

En una selección definida por el usuario, se puede determinar el alcance de la búsqueda y seleccionar todos los dispositivos, los dispositivos administrados o los dispositivos no asignados. Los parámetros de búsqueda se especifican en las condiciones. Una selección de dispositivos puede tener varias condiciones con diferentes parámetros de búsqueda. Puede, por ejemplo, crear dos condiciones y especificar intervalos IP diferentes en cada una de ellas. Una selección con varias condiciones muestra los dispositivos que cumplen con cualquiera de esas condiciones. Por el contrario, los parámetros de búsqueda especificados en una condición se superponen. Si una condición especifica tanto un intervalo IP como el nombre de una aplicación instalada, se mostrarán únicamente los dispositivos que tengan asignada una dirección IP de ese intervalo y que tengan instalada esa aplicación.

Ver la lista de dispositivos de una selección de dispositivos

Kaspersky Security Center Cloud Console le permite ver la lista de dispositivos contenidos en 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 dominio de Windows especificado.

- Grupo de administración

  Muestra los dispositivos incluidos en el grupo de administración especificado.

- Descripción

Texto ubicado en el campo **Descripción** de la sección **General** dentro de la ventana de propiedades del dispositivo.

Para describir el texto del campo **Descripción**, puede utilizar los siguientes caracteres:

- Dentro de una palabra:
  - *****. Sustituye una cadena de cualquier largo (es decir, con cualquier número de caracteres).

    Ejemplo:

    Para describir palabras como **Servidor** o **Servidores**, puede ingresar **Servidor***.
  - **?.** Sustituye un carácter individual.

    Ejemplo:

    Para describir palabras como **Window** o **Windows**, puede ingresar **Windo?**.

    La consulta no puede comenzar con un asterisco (*****) ni con un signo de interrogación (**?**).
- Para encontrar varias palabras:
  - Espacio. Muestra todos los dispositivos que tienen, en su descripción, alguna de las palabras indicadas.

    Ejemplo:

    Para encontrar una frase que contenga las palabras **secundario** o **virtual**, puede incluir la expresión **secundario virtual** en la consulta.
  - **+**. Si agrega el signo + antes de una palabra, todos los resultados de búsqueda contendrán esa palabra.

    Ejemplo:

    Para encontrar una frase que contenga las palabras **secundario** y **virtual**, ingrese la consulta **+secundario+virtual**.
  - **-**. Si agrega el signo - antes de una palabra, ningún resultado de búsqueda contendrá esa palabra.

    Ejemplo:

    Para encontrar una frase que contenga **secundario** y no contenga **virtual**, ingrese la consulta **+secundario-virtual**.
  - **"<cadena>"**. El texto que se ingresa entre comillas debe estar presente en el texto.

    Ejemplo:

    Para encontrar una frase que contenga la combinación de palabras **servidor secundario**, puede ingresar **"servidor secundario"** en la consulta.

- 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 sección **Active Directory**, puede configurar criterios para dispositivos incluidos en una selección según sus datos de Active Directory:

- **El dispositivo está en una unidad organizativa de Active Directory**

  Si activa esta opción, la selección incluirá los dispositivos de la unidad organizativa de Active Directory especificada en el campo de entrada.

  Esta opción está deshabilitada de manera predeterminada.

- **Incluir unidades organizativas secundarias**

  Si habilita esta opción, la selección incluirá los dispositivos de todas las unidades organizativas secundarias de la unidad organizativa de Active Directory especificada.

  Esta opción está deshabilitada de manera predeterminada.

- **Este dispositivo pertenece al grupo de Active Directory**

  Si habilita esta opción, la selección incluirá los dispositivos que pertenezcan al grupo de Active Directory especificado en el campo de entrada.

  Esta opción está deshabilitada de 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.

En la sección **Segmentos de la nube**, puede configurar criterios para incluir dispositivos en una selección según sus respectivos segmentos de nube:

- **El dispositivo está en un segmento de la nube**

  Si esta opción está habilitada, puede elegir dispositivos de los segmentos de nube de AWS, Azure y Google.

  Si también habilita la opción **Incluir objetos secundarios**, la búsqueda se realizará en todos los objetos secundarios del segmento elegido.

  Los resultados de la búsqueda solo incluirán aquellos dispositivos que estén en el segmento seleccionado.

- **Dispositivo descubierto mediante la API**

  La lista desplegable le permite operar con el hecho de que el dispositivo pueda detectarse con las herramientas provistas por una API.

  - **Sí**. El dispositivo se detecta mediante el uso de la API de AWS, Azure o Google.
  - **No**. El dispositivo no se puede detectar mediante el uso de la API de AWS, Azure o Google. Es decir, o bien el dispositivo no se encuentra en el entorno de nube, o bien sí está en el entorno de nube, pero, por algún motivo, no se lo puede detectar con una API.
  - Ningún valor. Esta condición no se aplica.

Estados de los dispositivos

En la sección **Estado del dispositivo administrado**, puede configurar criterios para incluir dispositivos en una selección según la descripción del estado de dispositivos desde una aplicación administrada:

- **Estado del dispositivo**

  Lista desplegable en la que puede seleccionar un estado de dispositivo: *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 (*Desconocido, 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 (*Desconocido*, *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 (*Desconocido, Detenido, Iniciando, En pausa, En ejecución, Fallo).*

- Estado de Endpoint Server

  Buscar dispositivos basándose en el estado del componente Sensor de Endpoint (*Desconocido, 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

  Nombre del dispositivo en la red de Windows. El dispositivo con el nombre especificado se incluirá en la selección.

- Descripción

  Descripción del dispositivo o unidad de hardware. Los dispositivos que tengan la descripción indicada en este campo se incluirán en la selección.

  Si desea agregar una descripción a un dispositivo, puede hacerlo (en cualquier formato) a través de la ventana de propiedades del mismo. El campo permite realizar búsquedas de texto completo.

- Proveedor del dispositivo

  Nombre del fabricante del dispositivo. Los dispositivos producidos por el fabricante especificado en este campo se incluyen en la selección.

  Puede ingresar el nombre del fabricante en la ventana de propiedades de un dispositivo.

- Número de serie

Todas las unidades de hardware con el número de serie especificado en este campo se incluirán en la selección.

- **Número de inventario**

  Los equipos que tengan el número de inventario indicado en este campo se incluirán en la selección.

- **Usuario**

  Todas las unidades de hardware del usuario especificado en este campo se incluirán en la selección.

- **Ubicación**

  Ubicación de un dispositivo o una unidad de hardware (por ejemplo, en la sede central o en una sucursal). 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**

  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**

  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**

  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

  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

  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

  Lista desplegable en la que puede seleccionar una aplicación. Los dispositivos que tengan instalada la aplicación elegida se incluirán en la selección.

- Versión de la aplicación

  Campo de entrada en el que puede especificar la versión de la aplicación seleccionada.

- Proveedor

  Lista desplegable en la que puede seleccionar el desarrollador de una aplicación instalada en el dispositivo.

- Estado de la aplicación

  Lista desplegable en la que puede seleccionar el estado de la aplicación (*Instalada*, *Sin instalar*). Se incluirán en la selección los dispositivos que tengan o no tengan (dependiendo del estado seleccionado) la aplicación seleccionada.

- Buscar por 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 aplicaciones

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

Lista desplegable en la que puede seleccionar el estado de la aplicación (*Instalada*, *Sin instalar*). Se incluirán en la selección los dispositivos que tengan o no tengan (dependiendo del estado seleccionado) la aplicación seleccionada.

En el campo de entrada, puede definir un criterio para incluir dispositivos en la selección cuando se realice una búsqueda basada en el nombre de una aplicación o en un número de paquete de actualización.

Si el campo queda en blanco, este criterio no se aplicará.

- Seleccione el período de la última actualización de módulos

  Use esta opción para definir un criterio que permita buscar dispositivos según la hora en que se hayan actualizado por última vez los módulos de las aplicaciones instaladas en ellos.

  Si activa esta casilla, podrá utilizar los campos de entrada para definir el intervalo de tiempo (fecha y hora) en el que deberá haber ocurrido la última actualización de módulos de las aplicaciones instaladas en los dispositivos.

  Si no activa esta casilla, no se aplicará este criterio.

  Esta casilla no está marcada de manera predeterminada.

- El dispositivo se administra a través del Servidor de administración

  En la lista desplegable, puede incluir en la selección los dispositivos administrados a través de Kaspersky Security Center Cloud Console:

  - **Sí**. La aplicación incluye en la selección los dispositivos administrados a través de Kaspersky Security Center Cloud Console.
  - **No**. La aplicación incluye dispositivos en la selección que Kaspersky Security Center Cloud Console no administra.
  - **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

  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*.

  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.

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.

- **Todos los dispositivos que tengan esta etiqueta**

  Si selecciona esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que lleven, en su descripción, la etiqueta seleccionada. La consulta de búsqueda puede incluir el asterisco, que representa una cadena de cualquier longitud (número de caracteres).

  Esta opción está seleccionada de manera predeterminada.

- **Todos los dispositivos que no tengan esta etiqueta**

  Si selecciona esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que no lleven en su descripción la etiqueta seleccionada. La consulta de búsqueda puede incluir el asterisco, que representa una cadena de cualquier longitud (número de caracteres).

Usuarios

En la sección **Usuarios**, puede configurar los criterios para incluir dispositivos en la selección basándose en las cuentas de usuario con las que se haya iniciado sesión en el sistema operativo.

- **Último usuario que inició sesión en el sistema**

  Si esta opción está habilitada, puede seleccionar la cuenta de usuario para configurar el criterio. Tenga en cuenta que la lista de usuarios se filtra y muestra los usuarios internos. Los resultados de la búsqueda incluyen los dispositivos en los que el usuario seleccionado ha realizado el último inicio de sesión en el sistema.

- **Usuario que inició sesión en el sistema al menos una vez**

  Si esta opción está habilitada, puede seleccionar la cuenta de usuario para configurar el criterio. Tenga en cuenta que la lista de usuarios se filtra y muestra los usuarios internos. Los resultados de la búsqueda incluyen los dispositivos en los que el usuario especificado haya iniciado sesión en el sistema al menos una vez.

Exportar la lista de dispositivos de una selección de dispositivos

Kaspersky Security Center Cloud Console 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**.

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.

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.

Acerca de los estados de los dispositivos

Kaspersky Security Center Cloud Console 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 Cloud Console tiene en cuenta el indicador de visibilidad del dispositivo en la red (consulte la tabla a continuación). Si Kaspersky Security Center Cloud Console 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.	• Interruptor activado. • Interruptor desactivado.
Demasiados virus detectados	Una tarea de detección de virus, por ejemplo, la tarea Análisis antivirus, detectó 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.	• Detenida. • En pausa. • En ejecución.
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 *Análisis de malware* 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 **Amenazas activas** 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.	• Interruptor desactivado. • Interruptor activado.
Se han detectado vulnerabilidades de software	El dispositivo es visible en la red y tiene instalado el Agente de red, pero la tarea *Buscar vulnerabilidades y actualizaciones requeridas* ha encontrado aplicaciones instaladas en el dispositivo que tienen vulnerabilidades con el nivel de gravedad especificado.	• Crítico. • Alto. • Medio. • Ignorar si la vulnerabilidad no se puede reparar. • Ignorar si hay una actualización asignada para instalarse.
La licencia comercial ha caducado	El dispositivo es visible en la red, pero la licencia ha caducado.	• Interruptor desactivado. • Interruptor activado.

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.
Hace mucho tiempo que no se comprueba si hay actualizaciones de Windows Update	El dispositivo es visible en la red, pero la tarea Realizar la sincronización de Windows Update no se ejecutó durante el intervalo de tiempo especificado.	Más de 1 día.
Estado de cifrado no válido	El Agente de red está instalado en el dispositivo, pero el resultado del cifrado del dispositivo es igual al valor especificado.	• No cumple con la directiva porque el usuario no dio su consentimiento (solo para dispositivos externos). • No cumple con la directiva debido a un error. • Se debe reiniciar el dispositivo al aplicar la directiva. • No se ha especificado una directiva de cifrado. • No compatible. • Al aplicar la directiva.
La configuración del dispositivo móvil no cumple la directiva	Los ajustes del dispositivo móvil no son los que se encontraron en la directiva de Kaspersky Endpoint Security for Android durante el chequeo de reglas de cumplimiento normativo.	• Interruptor desactivado. • Interruptor activado.
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.	• Interruptor desactivado. • Interruptor activado.
Estado del dispositivo definido por la aplicación	El estado del dispositivo es definido por la aplicación administrada.	• Interruptor desactivado. • Interruptor activado.
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 *Crítico* o *Advertencia* cambiarán por el estado *Sin inconvenientes* cuando el dispositivo se sincronice correctamente con el Servidor de administración y el espacio libre en el dispositivo supere o iguale el valor especificado.	Más de 0 MB.
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.	• Interruptor desactivado. • Interruptor activado.
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.	Más de 0 minutos.

	En este caso, el estado de la aplicación de seguridad es *detenida* o *error*, y difiere del siguiente: *iniciada*, *en ejecución* o *suspendida*.	
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.	• Interruptor desactivado. • Interruptor activado.

Kaspersky Security Center Cloud Console 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 configuradas. Si no se cumplen estas condiciones, el dispositivo cliente toma el estado *Sin inconvenientes*.

Cada estado puede corresponderse con distintos valores de una misma condición. De forma predeterminada, por ejemplo, cuando la condición **Las bases de datos están desactualizadas** tiene el valor **Más de 3 días**, se asigna el estado *Advertencia* al dispositivo cliente; si el valor es **Más de 7 días**, se asigna el estado *Crítico*.

Cuando Kaspersky Security Center Cloud Console 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.

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. En el paso **Configuración de tarea nueva**, especifique los siguientes ajustes:

a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Security Center Cloud Console**.

b. En el campo **Tipo de tarea**, seleccione **Cambiar Servidor de administración**.

c. En la ventana **Nombre de la tarea**, póngale un nombre a la tarea que está creando.

El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

d. Seleccione los dispositivos a los que se asignará la tarea.

- Asignar tarea a un grupo de administración

  La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

  Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

  Si se asigna una tarea a un grupo de administración, la pestaña **Seguridad** no se muestra en la ventana de propiedades de la tarea porque las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

- Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista

  Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

  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.

4. En el paso **Cobertura de la tarea**, especifique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

5. En el siguiente paso, confirme que acepta los términos de cambio del Servidor de administración para los dispositivos cliente.

6. En el siguiente paso, seleccione el Servidor de administración que desea utilizar para administrar los dispositivos seleccionados.

7. En el paso **Seleccionar una cuenta para ejecutar la tarea**, especifique la configuración 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.

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.

Evitar conflictos entre varios Servidores de administración

Si tiene más de un Servidor de administración en su red, pueden ver los mismos dispositivos cliente. Esto puede resultar, por ejemplo, en que el Servidor de administración instale una aplicación que ya fue instalada por otro Servidor de administración, y otros tipos de conflictos. Para evitar que una aplicación se instale en un dispositivo administrado por otro Servidor de administración, debe activar la opción **Instalar solo en dispositivos administrados a través de este Servidor de administración** en las propiedades de la tarea *Instalar aplicación en remoto*.

Si activa la opción **Instalar solo en dispositivos administrados a través de este Servidor de administración** y luego ejecuta la tarea *Instalar aplicación en remoto*, se realiza una verificación para determinar si los dispositivos están administrados por otro Servidor de administración. Para los dispositivos administrados por otro Servidor de administración, el valor del atributo **Administrado por otro Servidor de administración** se establecerá en `true`. La tarea *Instalar aplicación en remoto* no se aplicará a estos dispositivos.

Los valores del atributo **Administrado por otro Servidor de administración** se muestran en la columna **Administrado por otro Servidor de administración** en la lista de dispositivos administrados y la lista de dispositivos no asignados.

También puede usar la propiedad **Administrado por otro Servidor de administración** como criterio para los siguientes propósitos:

- Mostrar dispositivos administrados
- Selecciones de dispositivos
- Reglas de movimiento de dispositivos
- Reglas de etiquetado automático

Para restablecer el atributo Administrado por otro Servidor de administración,

En el menú principal de Kaspersky Security Center Cloud Console, vaya a **Detección y despliegue** → **Dispositivos no asignados**, seleccione el dispositivo requerido y luego haga clic en el botón **Eliminar el atributo Administrado por un Servidor de administración diferente**.

Se restablece el atributo **Administrado por otro Servidor de administración**.

Crear perfiles de conexión al Servidor de administración

Para permitir que los usuarios fuera de la oficina cambien el método de conexión del Agente de red al Servidor de administración, debe configurar los perfiles de conexión del Servidor de administración.

Los perfiles de conexión solo son compatibles con dispositivos que ejecutan Windows y MacOS.

Para crear un perfil de conexión, siga estos pasos:

1. En el menú principal, vaya a **Activos (dispositivos)** y realice una de las siguientes acciones:
   - Si desea crear un perfil de conexión para un grupo de dispositivos administrados, haga clic en **Directivas y perfiles** y, a continuación, en **Agente de red de Kaspersky Security Center**.
   - Si desea crear un perfil de conexión para un dispositivo administrado específico, haga clic en **Dispositivos administrados** y, a continuación, en el nombre del dispositivo. En la ventana que se abre, vaya a la pestaña **Aplicaciones** y, a continuación, haga clic en **Agente de red de Kaspersky Security Center**.

   Se abre la ventana de propiedades de la directiva del Agente de red.
2. Vaya a la pestaña **Configuración de la aplicación** y, luego, a la sección **Conectividad**.
3. En la sección **Perfiles de conexión**, haga clic en el botón **Configuración**.

   La subsección **Perfiles de conexión al Servidor de administración** muestra la tabla de perfiles de conexión.

   No puede ver, modificar ni eliminar los perfiles de conexión **Servicio de administración principal** y **Modo sin conexión**.
4. Haga clic en el botón **Añadir** y, luego, en la ventana que se abre, especifique el nombre del perfil.

El nombre debe ser exclusivo. No puede utilizar el mismo nombre para varios perfiles.

5. Si es necesario, marque las casillas de verificación en los siguientes campos:

   - **Activar modo Fuera de la oficina cuando el Servidor de administración no esté disponible**.
   - **Usar servidor proxy**.
     Si elige esta opción, siga estos pasos:
     - Especifique la información en los campos **Dirección** y **Número de puerto**.
     - Si es necesario, marque la casilla **Autenticación del servidor proxy** y, luego, especifique el nombre de usuario y la contraseña en los campos correspondientes.

6. Haga clic en el botón **Guardar**.

El nuevo perfil aparecerá en la tabla de perfiles de conexión. Puede usarlo al definir la **Configuración de las ubicaciones de red**.

La configuración de una ubicación de red define las características de la red con la cual está conectado el dispositivo cliente y especifica las reglas que hacen que el Agente de red cambie de un perfil de conexión de Servidor de administración a otro en respuesta a un cambio en las características de la red.

Puede editar y eliminar perfiles de conexión.

Para editar un perfil de conexión, haga lo siguiente:

1. En la tabla de perfiles de conexión, haga clic en el nombre del perfil de conexión que desea editar.
2. Realice todos los cambios necesarios y, a continuación, haga clic en el botón **Guardar**.

   Se aplicarán los cambios al perfil de conexión.

Para eliminar un perfil de conexión, haga lo siguiente:

1. En la tabla de perfiles de conexión, marque las casillas de verificación ubicadas junto a los perfiles de conexión que desea eliminar.
2. Haga clic en el botón **Eliminar**.

   Se eliminarán los perfiles de conexión elegidos.

Acerca de los clústeres y las matrices de servidores

Kaspersky Security Center Cloud Console 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 Cloud Console 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 Cloud Console 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.

Etiquetas de dispositivo

Kaspersky Security Center Cloud Console le permite etiquetar 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 Cloud Console 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, si su red incluye dispositivos que ejecutan Windows, Linux o macOS, puede configurar una regla que asignará la etiqueta `[Linux]` a todos los dispositivos basados en Linux. A continuación, puede usar esta etiqueta al crear una selección de dispositivos. Esto le ayudará a clasificar todos los dispositivos basados en Linux 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 de dispositivos**.
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 de dispositivos**.
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 de dispositivos**.
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 de dispositivos**.
2. Haga clic en el vínculo **Ver dispositivos** junto a una etiqueta para ver a qué dispositivos se la ha asignado.

   Se le redirigirá a la sección **Dispositivos administrados** del menú principal, donde verá los dispositivos filtrados según la etiqueta en la que haya hecho clic en el vínculo **Ver dispositivos**.
3. Para regresar a la lista de etiquetas de dispositivo, haga clic en el botón **Atrás** de su navegador.

Después de ver los dispositivos que tienen asignada la etiqueta, puede crear y asignar una nueva etiqueta o asignar la etiqueta existente a otros dispositivos. En este caso, debe eliminar el filtro por etiqueta, seleccionar los dispositivos y luego asignar la etiqueta.

Ver las etiquetas asignadas a un dispositivo

Para ver las etiquetas asignadas a un dispositivo:

1. En el menú principal, vaya a **Activos (dispositivos)**→ **Dispositivos administrados**.
2. Haga clic en el nombre del dispositivo cuyas etiquetas desee ver.
3. En la ventana que se abre, que contendrá las propiedades del dispositivo, elija la pestaña **Etiquetas**.

   Se muestra la lista de etiquetas asignadas al dispositivo seleccionado. En la columna **Etiqueta asignada**, puede ver cómo se asignó la etiqueta.

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.

También puede ver las etiquetas asignadas a un dispositivo en la línea de comando mediante la utilidad klscflag.

Para ver las etiquetas asignadas a un dispositivo en la línea de comando, ejecute el siguiente comando:

```
klscflag -ssvget -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -svt
ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

Etiquetar dispositivos manualmente

Para asignar una etiqueta a un dispositivo:

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.

Para asignar una etiqueta a varios dispositivos:

1. En el menú principal, vaya a **Activos (dispositivos)**→ **Dispositivos administrados**.
2. Seleccione los dispositivos a los que desea asignar una etiqueta.
3. Haga clic en **Etiquetas** y seleccione **Asignar** en la lista desplegable.
4. En la ventana que se abre, seleccione una etiqueta de la lista desplegable.
   Si es necesario, puede seleccionar varias etiquetas.
   Además, puede hacer lo siguiente:
   - Edite el nombre de una etiqueta haciendo clic en el icono **Editar** (✎).
     Especifique el nuevo nombre de la etiqueta y, luego, haga clic en el botón **Guardar**.

     Tenga en cuenta que también se cambiará el nombre de la etiqueta en la lista de etiquetas de dispositivo.
   - Elimine una etiqueta haciendo clic en el icono **Eliminar** (🗑).
     En la ventana que se abre, haga clic en **Eliminar**.

     Tenga en cuenta que la etiqueta también se eliminará del Servidor de administración.
5. Haga clic en el botón **Guardar**.

Se asignan las etiquetas a los dispositivos seleccionados. Puede eliminar las etiquetas asignadas.

Quitar etiquetas asignadas a un dispositivo

La etiqueta desasignada no se elimina. Si lo desea, puede eliminarla manualmente.

Las etiquetas asignadas a un dispositivo por una aplicación o por el Agente de red no se pueden eliminar manualmente. Para eliminar estas etiquetas, utilice la utilidad klscflag.

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 **¿Desea desasignar etiqueta?**.
6. En la ventana que se abre, haga clic en **Sí**.

El dispositivo pierde la etiqueta.

Para eliminar etiquetas de varios dispositivos:

1. En el menú principal, vaya a **Activos (dispositivos)**→ **Dispositivos administrados**.
2. Seleccione los dispositivos cuyas etiquetas desea eliminar.
3. Haga clic en **Etiquetas** y seleccione **Desasignar** en la lista desplegable.
4. En la ventana que se abre, seleccione las casillas de verificación junto a las etiquetas que desea eliminar.

   La ventana muestra todas las etiquetas asignadas a todos los dispositivos que seleccionó en el paso 2.

5. Haga clic en el botón **Guardar**.

Se eliminan las etiquetas de los dispositivos.

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 de dispositivos**, 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**: atributos de red del dispositivo (por ejemplo, el nombre del dispositivo en la red de Windows o su pertenencia a un dominio o a una subred IP).

     Si la intercalación de la distinción entre mayúsculas y minúsculas está configurada para la base de datos que usa para Kaspersky Security Center Cloud Console, 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.
   - **Active Directory**: presencia del dispositivo en una unidad organizativa o grupo de Active Directory.
   - **Registro de aplicaciones**: presencia de aplicaciones de distintos proveedores en el dispositivo.

7. Haga clic en **Aceptar** para guardar los cambios.

   Si es necesario, puede especificar varias condiciones para una misma regla. En ese caso, la etiqueta se asignará a cualquier dispositivo que cumpla con al menos una condición.

8. Haga clic en **Guardar** para guardar los cambios.

La nueva regla se aplicará a los dispositivos administrados del Servidor de administración seleccionado. Si la configuración de un dispositivo cumple con las condiciones de la regla, ese dispositivo recibirá la etiqueta.

Tras la ejecución inicial, la regla se aplicará en los siguientes casos:

- automática y periódicamente, atendiendo a la carga del servidor.

- cada vez que se edite la regla.
- cada vez que la regla se aplique manualmente.
- cada vez que el Servidor de administración detecte un cambio en la configuración de un dispositivo que reúna las condiciones de la regla o en la configuración de un grupo que contenga dicho dispositivo.

Puede crear más de una regla de etiquetado. Si crea varias reglas de etiquetado y un dispositivo cumple simultáneamente con las condiciones de todas ellas, dicho dispositivo recibirá varias etiquetas. Puede ver la lista de todas las etiquetas asignadas a un dispositivo en las propiedades del mismo.

Ejecución de reglas para etiquetar dispositivos automáticamente

Cuando se ejecuta una regla, la etiqueta definida en las propiedades de la misma se asigna a los dispositivos que reúnen las condiciones especificadas en las propiedades de esa misma regla. Solo es posible ejecutar reglas activas.

Para ejecutar reglas de etiquetado automático de dispositivos:

1. Vea las reglas de etiquetado automático de dispositivos.
2. Active las casillas de verificación ubicadas junto a las reglas activas que quiera ejecutar.
3. Haga clic en el botón **Ejecutar regla**.

   Se ejecutan las reglas seleccionadas.

Eliminación de una regla para etiquetar dispositivos automáticamente

Para eliminar una regla de etiquetado automático de dispositivos:

1. Vea las reglas de etiquetado automático de dispositivos.
2. 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.

Cuarentena y Copia de seguridad

Como resultado de un análisis, las aplicaciones antivirus de Kaspersky instaladas en los dispositivos cliente pueden poner archivos en Cuarentena o en Copia de seguridad.

Cuarentena es un repositorio especial en el que se almacenan aquellos archivos que probablemente estén infectados con virus y aquellos que no se pueden desinfectar al momento de la detección.

Copia de seguridad se ha diseñado para almacenar copias de seguridad de los archivos que se eliminan o modifican durante el proceso de desinfección.

Kaspersky Security Center Cloud Console crea una lista resumida de los archivos puestos en Cuarentena o en Copia de seguridad por la aplicación Kaspersky en los dispositivos. El Agente de red de cada dispositivo cliente se comunica con el Servidor de administración para transmitirle información sobre los archivos en Cuarentena y Copia de seguridad.

Kaspersky Security Center Cloud Console no copia archivos de los repositorios al Servidor de administración. Los archivos quedan almacenados en los repositorios de los dispositivos.

Descargar un archivo desde los repositorios

Kaspersky Security Center Cloud Console le permite descargar copias de los archivos que la aplicación de seguridad ha puesto en Cuarentena o en Copia de seguridad en un dispositivo cliente. Los archivos se copian en el destino que especifique.

Puede descargar archivos solo si se cumple una de las siguientes condiciones: la opción **No desconectar del Servidor de administración** está activada en la configuración del dispositivo, un servidor push está en uso o una puerta de enlace de conexión está en uso. De lo contrario, la descarga no es posible.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

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.

Eliminar archivos de los repositorios

Para eliminar un archivo de Cuarentena o 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 eliminar y haga clic en **Eliminar**.

3. Confirme que desea eliminar el archivo.

La aplicación de seguridad en el dispositivo cliente que haya puesto los archivos en el repositorio (Cuarentena o Copia de seguridad) los eliminará del mismo.

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) → Grupos → <nombre del grupo> → 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 pestaña **Avanzado**, 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 habilitar o deshabilitar el seguimiento.

   Se abre la lista de opciones de diagnóstico remoto.

4. Si desea habilitar el seguimiento, haga lo siguiente:

   a. En la sección **Seguimiento**, haga clic en **Activar seguimiento**.

   b. En la ventana **Modificar nivel de seguimiento**, recomendamos que mantenga los valores de configuración predeterminados. De ser necesario, un especialista del servicio de soporte técnico le indicará cómo modificar la configuración. Las opciones de configuración disponibles son las siguientes:

   - **Nivel de seguimiento**

     El nivel de seguimiento determina qué tan detallado es el archivo de seguimiento.

   - **Seguimiento 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 Kaspersky Security Agent está regulado por la configuración del Agente de red. Por lo tanto, las opciones **Activar seguimiento** y **Modificar nivel de seguimiento** están desactivadas para este componente en los dispositivos cliente que ejecutan Linux.

5. Para deshabilitar el seguimiento para la aplicación seleccionada, haga clic en **Desactivar seguimiento**.

   Se deshabilita el seguimiento para la aplicación seleccionada.

Habilitar el seguimiento con Xperf

Si utiliza Kaspersky Endpoint Security, un especialista de nuestro servicio de soporte técnico podría pedirle que habilite el seguimiento con Xperf. Esta función permite obtener información sobre el rendimiento del sistema.

Para habilitar y configurar el seguimiento 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 **Seguimiento de Xperf**, haga clic en **Activar seguimiento de Xperf**.

   Si el seguimiento con Xperf ya está habilitado, verá, en cambio, el botón **Desactivar seguimiento 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 seguimiento de Xperf** en la sección **Seguimiento de Xperf**.

   Se deshabilita el seguimiento con Xperf.

Descargar los archivos de seguimiento de una aplicación

Puede descargar archivos de seguimiento desde un dispositivo cliente solo si se cumple una de las siguientes condiciones: la opción **No desconectar del Servidor de administración** está activada en la configuración del dispositivo, un servidor push está en uso o una puerta de enlace de conexión está en uso. De lo contrario, la descarga no es posible.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

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 **Seguimiento**, haga clic en el botón **Archivos de seguimiento**.

   Se abre la ventana **Registros de seguimiento del dispositivo**, en la que se muestra una lista de archivos de seguimiento.
5. En la lista de archivos de seguimiento, seleccione el archivo que desea descargar.
6. Realice una de las siguientes acciones:

   - Descargue el archivo seleccionado haciendo 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.

   Se abre la ventana **Registros de seguimiento del dispositivo**, en la que se muestra una lista de archivos de seguimiento.
4. En la lista de archivos de seguimiento, seleccione uno o varios archivos que desee eliminar.
5. Haga clic en el botón **Eliminar**.

Los archivos de seguimiento seleccionados quedan eliminados.

Descargar la configuración de las aplicaciones

Puede descargar la configuración de la aplicación desde un dispositivo cliente solo si se cumple una de las siguientes condiciones: la opción **No desconectar del Servidor de administración** está activada en la configuración del dispositivo, un servidor push está en uso o una puerta de enlace de conexión está en uso. De lo contrario, la descarga no es posible.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

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

Puede descargar información del sistema a su dispositivo desde un dispositivo cliente solo si se cumple una de las siguientes condiciones: la opción **No desconectar del Servidor de administración** está activada en la configuración del dispositivo, un servidor push está en uso o una conexión La puerta de enlace está en uso. De lo contrario, la descarga no es posible.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

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.

El archivo con la información se descarga en la ubicación especificada.

Descargar registros de eventos

Puede descargar registros de eventos a su dispositivo desde un dispositivo cliente solo si se cumple una de las siguientes condiciones: la opción **No desconectar del Servidor de administración** está activada en la configuración del dispositivo, un servidor push está en uso o una conexión La puerta de enlace está en uso. De lo contrario, la descarga no es posible.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

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.
     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.

Realizar un diagnóstico remoto de una aplicación y descargar los resultados

Para realizar un diagnóstico de una aplicación instalada 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 la aplicación para la que desee realizar el diagnóstico remoto.

   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.

Si desea ejecutar un script personalizado en el dispositivo cliente, puede usar la variable de entorno `KLACDT_SAVE_SETTING` para determinar la ruta donde se guardarán los resultados de la ejecución. Por ejemplo:

- Para un dispositivo Windows:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- Para un dispositivo Linux:

  ```
  repetir algún resultado > $KLACDT_SAVE_SETTING/res.log
  ```

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 el campo **Tipo de objeto**, elija el tipo de objeto que desea cargar:
   - Elija **Archivo** para cargar el archivo ejecutable.
   - Elija **Carpeta** para cargar la carpeta que contiene la aplicación que desea ejecutar en el dispositivo cliente.

Si elige este tipo de objeto, aparecerá el campo **Nombre del archivo ejecutable que debe ejecutarse**. En este campo, especifique el nombre del archivo ejecutable en la carpeta. También puede especificar la ruta relativa al archivo.

- Elija **Archivo comprimido** para cargar el archivo comprimido ZIP que contiene la aplicación que desea ejecutar en el dispositivo cliente.

  Si elige este tipo de objeto, aparecerá el campo **Nombre del archivo ejecutable que debe ejecutarse**. En este campo, en la carpeta especifique el nombre del archivo ejecutable que desea ejecutar en el dispositivo cliente. También puede especificar la ruta relativa al archivo.

  El archivo ZIP debe incluir la carpeta de la utilidad. Esta carpeta contiene el archivo ejecutable que se ejecutará en un dispositivo remoto.

4. Cargue el objeto al elegirlo en la ventana del sistema o arrastrándolo al campo de carga.
5. Si es necesario, en el campo **Argumentos de la línea de comandos**, especifique los argumentos de la línea de comando que se pasarán al ejecutar el archivo ejecutable.
6. Haga clic en el botón **Cargar y ejecutar** para ejecutar la aplicación elegida en un dispositivo cliente.
7. Después de completar correctamente la ejecución de la aplicación, descargue los resultados de la ejecución haciendo clic en el botón **Descargar los resultados de la ejecución de la aplicación**.

   Los resultados de la ejecución de la aplicación se almacenan hasta que ejecute un nuevo diagnóstico o cierre la ventana.

Se completa el diagnóstico remoto del dispositivo cliente mediante la aplicación.

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.

Conexión remota al escritorio de un dispositivo cliente

Puede obtener acceso remoto al escritorio de un dispositivo cliente mediante el Agente de red instalado en el dispositivo. El Agente de red permite conectarse incluso si el dispositivo cliente tiene cerrados los puertos TCP y UDP.

Cuando se establece una conexión con el dispositivo, usted obtiene acceso total a la información almacenada en dicho dispositivo, de modo que podrá administrar las aplicaciones que haya instaladas en él.

Las conexiones remotas deben estar permitidas por el sistema operativo del dispositivo administrado al que pretenda acceder. En Windows 10, por ejemplo, debe estar habilitada la opción **Permitir conexiones de Asistencia remota a este equipo**, que se encuentra en **Panel de control → Sistema y seguridad → Sistema → Configuración de Acceso remoto**. Si tiene una licencia para la función Administración de vulnerabilidades y parches, puede activar esta opción de forma forzada cuando establece una conexión con un dispositivo administrado. Si no tiene una licencia para esta función, habilite la opción de manera local en el dispositivo administrado. No podrá establecer una conexión remota si esta opción está deshabilitada.

Para conectarse a un dispositivo remoto, debe contar con dos utilidades:

- La utilidad klsctunnel, desarrollada por Kaspersky. Esta utilidad debe almacenarse en su estación de trabajo. Se utiliza para conectar el Servidor de administración con el dispositivo cliente a través de un túnel.

  Kaspersky Security Center Cloud Console permite conexiones tunelizadas de TCP desde la Consola de administración mediante el Servidor de administración y, luego, mediante el Agente de red a un puerto especificado en un dispositivo administrado. Gracias a este túnel, una aplicación cliente instalada en el mismo dispositivo que la Consola de administración puede conectarse a un puerto TCP de un dispositivo administrado incluso si no existe una vía de conexión directa entre la Consola de administración y ese dispositivo administrado.

  La conexión entre el Servidor de administración y el dispositivo cliente remoto se debe hacer pasar por un túnel cuando el puerto que se utiliza para conectarse al Servidor de administración no está disponible en el dispositivo. El puerto del dispositivo podría no estar disponible en estos casos:

  - el dispositivo remoto está conectado a una red local en la que se utiliza el mecanismo NAT;
  - el dispositivo remoto está en la misma red local que el Servidor de administración, pero el puerto se ha cerrado con un firewall.

- El componente Conexión a Escritorio remoto, que forma parte de Microsoft Windows. La conexión con el escritorio remoto se establece a través de mstsc.exe, una utilidad que viene incluida en Windows, conforme a los ajustes de la utilidad.

  Si se conecta a la sesión de escritorio remoto establecida por un usuario, lo hará sin que el usuario lo sepa. Cuando usted se conecta a la sesión, el usuario del dispositivo se desconecta de la sesión sin previo aviso.

Para conectarse al escritorio de un dispositivo cliente, se debe cumplir una de las siguientes condiciones:

- El dispositivo cliente es miembro de un grupo de administración que tiene un punto de distribución con la opción **No desconectarse del Servidor de Administración** habilitada.
- En la configuración del dispositivo cliente, la opción **No desconectarse del Servidor de Administración** está habilitada.

  La cantidad máxima total de dispositivos cliente con la opción **No desconectarse del Servidor de Administración** habilitada es 300.

Para conectarse al escritorio de un dispositivo cliente:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados.**
2. Active la casilla de verificación ubicada junto al nombre del dispositivo al que desee acceder.
3. Haga clic en el botón **Conectar con el escritorio remoto**.

   Se abre la ventana Conectar con el escritorio remoto.
4. Haga clic en el botón **Descargar** para descargar la utilidad klsctunnel.
5. Haga clic en el botón **Copiar al portapapeles** para copiar el contenido del campo de texto. El contenido del campo es un objeto binario (denominado "BLOB", por el nombre de este tipo de objeto en inglés). El objeto contiene los parámetros que se necesitan para establecer la conexión entre el Servidor de administración y el dispositivo administrado.

   > Los BLOB tienen una validez de tres minutos. Si el suyo caduca, vuelva a abrir la ventana Conectar con el escritorio remoto para generar un nuevo BLOB.
6. Ejecute la utilidad klsctunnel.

   Se abre la ventana de la utilidad.
7. En el campo de texto, pegue el contenido que copió en el paso anterior.
8. Si utiliza un servidor proxy, active la casilla **Usar servidor proxy** y especifique los ajustes de conexión del servidor proxy.
9. Haga clic en el botón **Abrir puerto**.

   Se abre la ventana de inicio de sesión de Conexión a Escritorio remoto.
10. Especifique las credenciales de la cuenta con la que ha iniciado sesión actualmente en Kaspersky Security Center Cloud Console.
11. Haga clic en el botón **Conectar**.

Una vez que se establezca la conexión con el dispositivo, tendrá acceso al escritorio a través de la ventana Conexión a Escritorio remoto de Microsoft Windows.

Conectarse a un dispositivo a través de Windows Desktop Sharing

Puede obtener acceso remoto al escritorio de un dispositivo cliente mediante el Agente de red instalado en el dispositivo. El Agente de red permite conectarse incluso si el dispositivo cliente tiene cerrados los puertos TCP y UDP.

Puede conectarse a una sesión existente en un dispositivo cliente sin desconectar al usuario que la está utilizando. En ese caso, tanto usted como el usuario de la sesión del dispositivo comparten el acceso al escritorio.

Para conectarse a un dispositivo remoto, debe contar con dos utilidades:

- La utilidad klsctunnel, desarrollada por Kaspersky. Esta utilidad debe almacenarse en su estación de trabajo. Se utiliza para conectar el Servidor de administración con el dispositivo cliente a través de un túnel.

Kaspersky Security Center Cloud Console permite conexiones tunelizadas de TCP desde la Consola de administración mediante el Servidor de administración y, luego, mediante el Agente de red a un puerto especificado en un dispositivo administrado. Gracias a este túnel, una aplicación cliente instalada en el mismo dispositivo que la Consola de administración puede conectarse a un puerto TCP de un dispositivo administrado incluso si no existe una vía de conexión directa entre la Consola de administración y ese dispositivo administrado.

La conexión entre el Servidor de administración y el dispositivo cliente remoto se debe hacer pasar por un túnel cuando el puerto que se utiliza para conectarse al Servidor de administración no está disponible en el dispositivo. El puerto del dispositivo podría no estar disponible en estos casos:

- el dispositivo remoto está conectado a una red local en la que se utiliza el mecanismo NAT;
- el dispositivo remoto está en la misma red local que el Servidor de administración, pero el puerto se ha cerrado con un firewall.

- Windows Desktop Sharing. Al conectarse a una sesión existente del escritorio remoto, el usuario de la sesión del dispositivo recibe una solicitud de usted para establecer la conexión. No se guardará ninguna información sobre la actividad en remoto del dispositivo ni de sus resultados en los informes creados por Kaspersky Security Center Cloud Console.

  Puede configurar una auditoría de la actividad del usuario en un dispositivo cliente remoto. Durante la auditoría, la aplicación guarda información sobre los archivos del dispositivo cliente que el administrador haya abierto o modificado.

Para que pueda conectarse al escritorio de un dispositivo cliente a través de Windows Desktop Sharing, se deben cumplir las siguientes condiciones:

- Microsoft Windows Vista o posterior está instalado en su estación de trabajo.

  Para verificar si la función Uso compartido del escritorio de Windows está incluida en su edición de Windows, asegúrese de que CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} esté incluido en el registro de 32 bits.

- El dispositivo cliente debe tener Microsoft Windows Vista o una versión de Windows posterior.

- Kaspersky Security Center Cloud Console usa una licencia para la Administración de vulnerabilidades y parches.

- El dispositivo cliente es miembro de un grupo de administración que tiene un punto de distribución con la opción **No desconectarse del Servidor de Administración** habilitada o esta opción está habilitada en la configuración del dispositivo cliente.

  Tenga en cuenta que la cantidad máxima total de dispositivos cliente con la opción **No desconectarse del Servidor de Administración** habilitada es 300.

Para conectarse al escritorio de un dispositivo cliente a través de Escritorio compartido de Windows:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.
2. Active la casilla de verificación ubicada junto al nombre del dispositivo al que desee acceder.
3. Haga clic en el botón **Escritorio compartido de Windows**.

   El asistente de Escritorio compartido de Windows se abre.
4. Haga clic en el botón **Descargar** para obtener la utilidad klsctunnel. Espere a que se complete la descarga.

   Si ya tiene el archivo de la utilidad, omita este paso.
5. Haga clic en el botón **Siguiente**.

6. Elija una sesión abierta en el dispositivo al que desee conectarse. A continuación, haga clic en el botón **Siguiente**.

7. En el dispositivo de destino, se abrirá un cuadro de diálogo para que el usuario autorice la sesión de escritorio compartido. La sesión no comenzará sin el consentimiento del usuario.

   Después de que el usuario del dispositivo confirma la sesión de uso compartido de escritorio, se abre la siguiente página del asistente.

8. Haga clic en el botón **Copiar al portapapeles** para copiar el contenido del campo de texto. El contenido del campo es un objeto binario (denominado "BLOB", por el nombre de este tipo de objeto en inglés). El objeto contiene los parámetros que se necesitan para establecer la conexión entre el Servidor de administración y el dispositivo administrado.

   > Los BLOB tienen una validez de tres minutos. Si su BLOB caduca, genere uno nuevo.

9. Ejecute la utilidad klsctunnel.

   Se abre la ventana de la utilidad.

10. En el campo de texto, pegue el contenido que copió en el paso anterior.

11. Si utiliza un servidor proxy, active la casilla **Usar servidor proxy** y especifique los ajustes de conexión del servidor proxy.

12. Haga clic en el botón **Abrir puerto**.

    La sesión de escritorio compartido se abre en una nueva ventana. Si necesita interactuar con el dispositivo, haga clic en el ícono de menú ( ) ubicado en la esquina superior izquierda de la ventana y seleccione **Modo interactivo**.

Activación de reglas en modo Aprendizaje inteligente

Esta sección proporciona información sobre las detecciones realizadas en los dispositivos cliente por las reglas del Control de anomalías adaptativo de Kaspersky Endpoint Security para Windows.

Las reglas detectan y pueden bloquear comportamientos anómalos en los dispositivos cliente. Si las reglas funcionan en el modo Aprendizaje inteligente, detectan un comportamiento anómalo y envían informes sobre cada incidente al Servidor de administración de Kaspersky Security Center Cloud Console. La información transmitida se almacena en forma de lista en la subcarpeta **Activación de reglas en el estado Aprendizaje inteligente** de la carpeta **Repositorios**. Puede confirmar que las detecciones son válidas o agregarlas como exclusiones para que el tipo de comportamiento deje de considerarse anómalo.

La información sobre las detecciones se almacena en el registro de eventos del Servidor de administración (junto con otros eventos) y en el informe del Control de anomalías adaptativo.

Para obtener más información sobre el Control de anomalías adaptativo, las reglas, sus modos y estados, consulte la Ayuda de Kaspersky Endpoint Security.

Cómo ver la lista de detecciones realizadas con las reglas del Control de anomalías adaptativo

Para ver la lista de detecciones realizadas por las reglas del Control de anomalías adaptativo:

1. En el menú principal, vaya a **Operaciones** → **Repositorios**.
2. Haga click en el enlace **Activación de reglas en el estado Aprendizaje inteligente**.

   La lista muestra la siguiente información sobre las detecciones realizadas con las reglas del Control de anomalías adaptativo:

   - **Grupo de administración**

     El nombre del grupo de administración al que pertenece el dispositivo.

   - **Nombre del dispositivo**

     El nombre del dispositivo cliente en el que se aplicó la regla.

   - **Nombre**

     El nombre de la regla que se aplicó.

   - **Estado**

     Excluyendo. Este estado indica que el administrador procesó el elemento y lo agregó como exclusión a las reglas. El estado se mantiene hasta la siguiente sincronización del dispositivo cliente con el Servidor de administración; después de la sincronización, el elemento desaparece de la lista.

     Confirmando. Este estado indica que el administrador procesó y confirmó el elemento. El estado se mantiene hasta la siguiente sincronización del dispositivo cliente con el Servidor de administración; después de la sincronización, el elemento desaparece de la lista.

     Si no se muestra ningún valor, el administrador no ha procesado el elemento.

   - **Nombre de usuario**

     El nombre del usuario del dispositivo cliente que ejecutó el proceso que generó la detección.

   - **Procesado**

     Fecha en la que se detectó la anomalía.

   - **Ruta del proceso de origen**

     Ruta al proceso de origen, es decir, al proceso que realiza la acción (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

   - **Hash del proceso de origen**

     Hash SHA256 del archivo del proceso de origen (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del objeto de origen**

  Ruta al objeto que inició el proceso (para obtener más información, haga referencia a la ayuda de Kaspersky Endpoint Security).

- **Hash del objeto de origen**

  Hash SHA256 del archivo de origen (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del proceso de destino**

  Ruta al proceso de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del proceso de destino**

  Hash SHA256 del archivo de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del objeto de destino**

  Ruta al objeto de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del objeto de destino**

  Hash SHA256 del archivo de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

Para ver las propiedades de cada elemento de información:

1. En el menú principal, vaya a **Operaciones** → **Repositorios**.
2. Haga click en el enlace **Activación de reglas en el estado Aprendizaje inteligente**.
3. En la ventana que se abre, seleccione el objeto que desee.
4. Haga click en el enlace **Propiedades**.

   Se abre la ventana de propiedades del objeto y muestra información sobre el elemento seleccionado.

Puede confirmar o excluir cualquier elemento que aparezca en la lista de detecciones de las reglas del Control de anomalías adaptativo.

Para confirmar un elemento,

Seleccione un elemento (o varios elementos) en la lista de detecciones y haga clic en el botón **Confirmar**.

El estado del elemento (o de los elementos) cambiará a **Confirmando**.

Su confirmación contribuirá a las estadísticas utilizadas por las reglas (para obtener más información, consulte la documentación de Kaspersky Endpoint Security para Windows).

Para agregar un elemento como exclusión,

Seleccione un elemento (o varios elementos) en la lista de detecciones y haga clic en el botón **Excluir**.

Se inicia el Asistente para añadir exclusiones. Siga las instrucciones del asistente.

Si rechaza o confirma un elemento, se lo excluirá de la lista de detecciones la siguiente vez que el dispositivo cliente se sincronice con el Servidor de administración. El elemento dejará de aparecer en la lista.

Adición de exclusiones para las reglas del Control de anomalías adaptativo

El Asistente para añadir exclusiones le permite añadir exclusiones de las reglas de Control de anomalías adaptativo para Kaspersky Endpoint Security para Windows.

Para iniciar el Asistente para añadir exclusiones a través del nodo Control de anomalías adaptativo:

1. En el menú principal, vaya a **Operaciones → Repositorios → Activación de reglas en el estado Aprendizaje inteligente**.
2. En la ventana que aparece, elija uno o varios elementos de la lista de detecciones y haga clic en el botón **Excluir**.

   Puede agregar hasta 1000 exclusiones a la vez. Si selecciona más elementos e intenta agregarlos a las exclusiones, verá un mensaje de error.

Se inicia el Asistente para añadir exclusiones. Avance por el asistente utilizando el botón **Next**.

Administrar grupos de administración

Esta sección proporciona información sobre cómo administrar grupos de administración.

Se pueden realizar las siguientes acciones en los grupos de administración:

- Agregar cualquier número de grupos anidados de cualquier nivel de jerarquía a los grupos de administración.
- Agregar dispositivos a grupos de administración.
- Cambiar la jerarquía de los grupos de administración moviendo los dispositivos individuales y los grupos enteros a otros grupos.
- Eliminar los grupos anidados y los dispositivos de los grupos de administración.
- Agregar Servidores de administración secundarios y virtuales a los grupos de administración.
- Mover los dispositivos de los grupos de administración de un Servidor de administración a los de otro Servidor.

- Definir qué aplicaciones de Kaspersky serán automáticamente instaladas en los dispositivos incluidos en un grupo.

Puede realizar estas acciones solo si tiene el permiso **Modificar** en el área **Administración de grupos de administración** para los grupos de administración que desea administrar o para el Servidor de administración al que pertenecen estos grupos.

Creación de grupos de administración

Al principio, la jerarquía de los grupos de administración solo contiene un grupo de administración llamado grupo de **Dispositivos administrados**. Puede añadir dispositivos y subgrupos al grupo **Dispositivos administrados**.

Para crear un grupo de administración:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. En la jerarquía, seleccione el grupo de administración que se incluirá al nuevo grupo de administración.
3. Haga clic en el botón **Añadir**.
4. En la ventana que se abra, introduzca un nombre para el grupo y haga clic en **Añadir**.

   Aparece un nuevo grupo de administración con el nombre especificado en la jerarquía de los grupos de administración.

La aplicación permite crear una jerarquía de grupos de administración basada en la estructura de Active Directory o en la estructura de la red del dominio. También es posible crear una estructura de grupos a partir de un archivo de texto.

Para crear una estructura de grupos de administración:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. Haga clic en el botón **Importar**.

   Se inicia el Asistente de nueva estructura de grupos de administración. Siga las instrucciones del asistente.

Instalación automática de aplicaciones en dispositivos de un grupo de administración

Puede especificar qué paquetes de instalación deben utilizarse para la instalación remota automática de aplicaciones Kaspersky en dispositivos cliente de un grupo de administración.

Para configurar la instalación automática de las aplicaciones en dispositivos nuevos de un grupo de administración:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos** y haga clic en el nombre del grupo de administración requerido.
2. En la ventana que se abre, vaya a la pestaña **Instalación automática**.

3. Seleccione los paquetes de instalación de las aplicaciones que desea instalar en los dispositivos y haga clic en el botón **Guardar**.

   Si selecciona varios paquetes de instalación de la misma aplicación que difieren solo en sus versiones, se guarda el paquete de instalación con la última versión.

Después de seleccionar los paquetes de instalación, se crea un grupo de tareas para la instalación de las aplicaciones en los dispositivos del grupo de administración para cada una de las aplicaciones. Estas tareas se ejecutan en los dispositivos cliente inmediatamente después de que se agregan al grupo de administración.

Traslado de grupos de administración

Puede mover grupos de administración anidados dentro de la jerarquía de grupos.

Un grupo de administración se mueve junto con todos sus grupos anidados, Servidores de administración secundarios, dispositivos, directivas de grupo y tareas. El sistema aplicará al grupo toda la configuración correspondiente a su nueva posición en la jerarquía de los grupos de administración.

El nombre del grupo debe ser único dentro de un nivel de la jerarquía. Si ya existe un grupo con el mismo nombre en la carpeta a la que está trasladando el grupo de administración, debe cambiar el nombre de este último. Si no cambió el nombre del grupo que se moverá, cuando lo mueva, automáticamente se agregará un índice en formato **(<siguiente número de la secuencia>)** al nombre, por ejemplo: **(1)**, **(2)**.

No puede cambiar de nombre ni mover el grupo **Dispositivos administrados**.

Para mover un grupo de administración a otro nivel de la jerarquía de grupos de administración:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos** y luego marque la casilla junto al grupo de administración que desea mover.

2. En la barra de herramientas, haga clic en el botón **Mover**.

3. En la ventana que aparece, seleccione adónde desea mover el grupo de administración y haga clic en el botón **Mover**.

   La ventana se cierra y el grupo de administración se mueve a otro nivel de la jerarquía de grupos.

Eliminación de grupos de administración

Si elimina un grupo de administración que contiene Servidores de administración secundarios, grupos anidados, dispositivos cliente, tareas de grupo o directivas creadas para este grupo, también se eliminarán todos ellos.

Antes de eliminar el grupo de administración, debe eliminar todos los Servidores de administración secundarios, grupos anidados y dispositivos cliente de ese grupo.

Para eliminar un grupo de administración:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos** y luego seleccione la casilla de verificación junto al grupo de administración que desea eliminar.

2. En la línea del menú, haga clic en el botón **Eliminar**.

El grupo de usuario queda eliminado.

Directivas y perfiles de directivas

En Kaspersky Security Center Cloud 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

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

Estado de la directiva

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

Las directivas funcionan de acuerdo con las siguientes reglas:

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

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

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

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

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

- Un perfil de directiva entra en vigor cuando se cumple una condición de activación específica.

- Los perfiles de directivas contienen valores de configuración que difieren de los especificados en la directiva.
- La activación de un perfil de directiva modifica los ajustes vigentes del dispositivo administrado.
- Una directiva puede tener un máximo de 100 perfiles de directiva.

No puede crear una directiva del Servidor de administración.

Acerca del candado y el bloqueo de ajustes

Cada ajuste de configuración disponible en una directiva tiene un interruptor de bloqueo acompañado de un candado de ícono (). En la siguiente tabla, se muestran los estados que puede tener el interruptor de bloqueo.

Estados del interruptor de bloqueo

Estado	Descripción
Sin definir	Cuando un ajuste tiene un candado abierto a su lado y el interruptor de bloqueo está desactivado, el valor de dicho ajuste no se especifica a través de la directiva. El usuario puede modificar el valor del ajuste mediante la interfaz de la aplicación administrada. Estos ajustes se consideran *desbloqueados*.
Aplicar	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:

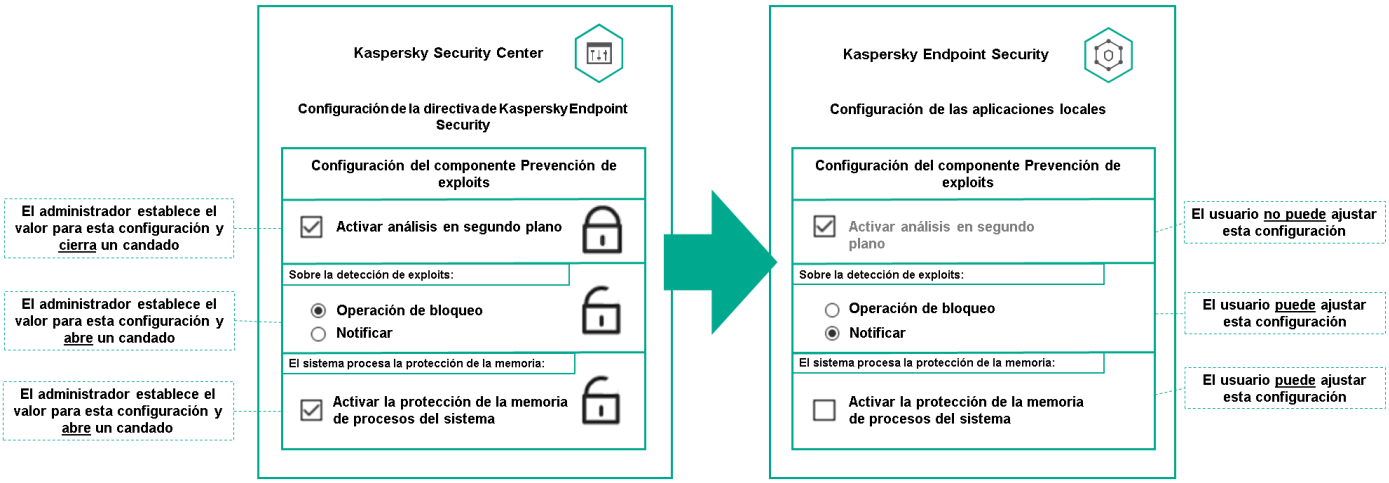
- Bloquear ajustes en la directiva de un subgrupo de administración
- Bloquear los ajustes de una aplicación de Kaspersky instalada en un dispositivo administrado

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

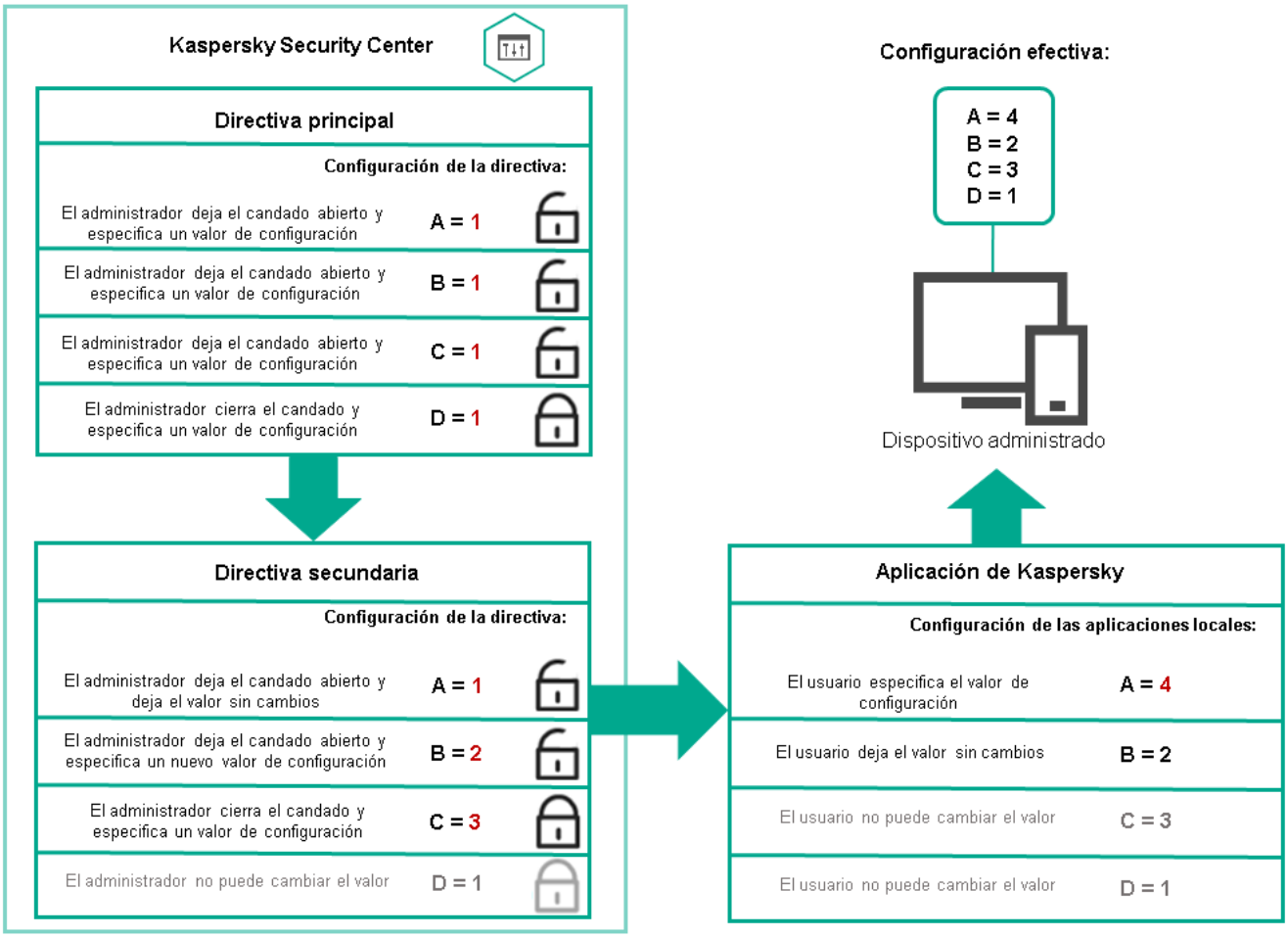
Si distintos dispositivos necesitan diferentes configuraciones, puede organizar los dispositivos en grupos de administración.

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).

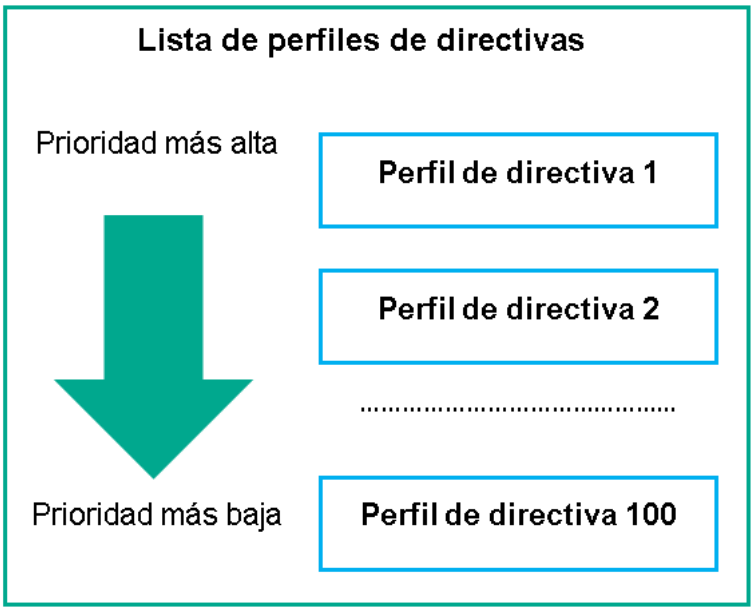


Jerarquía de directivas

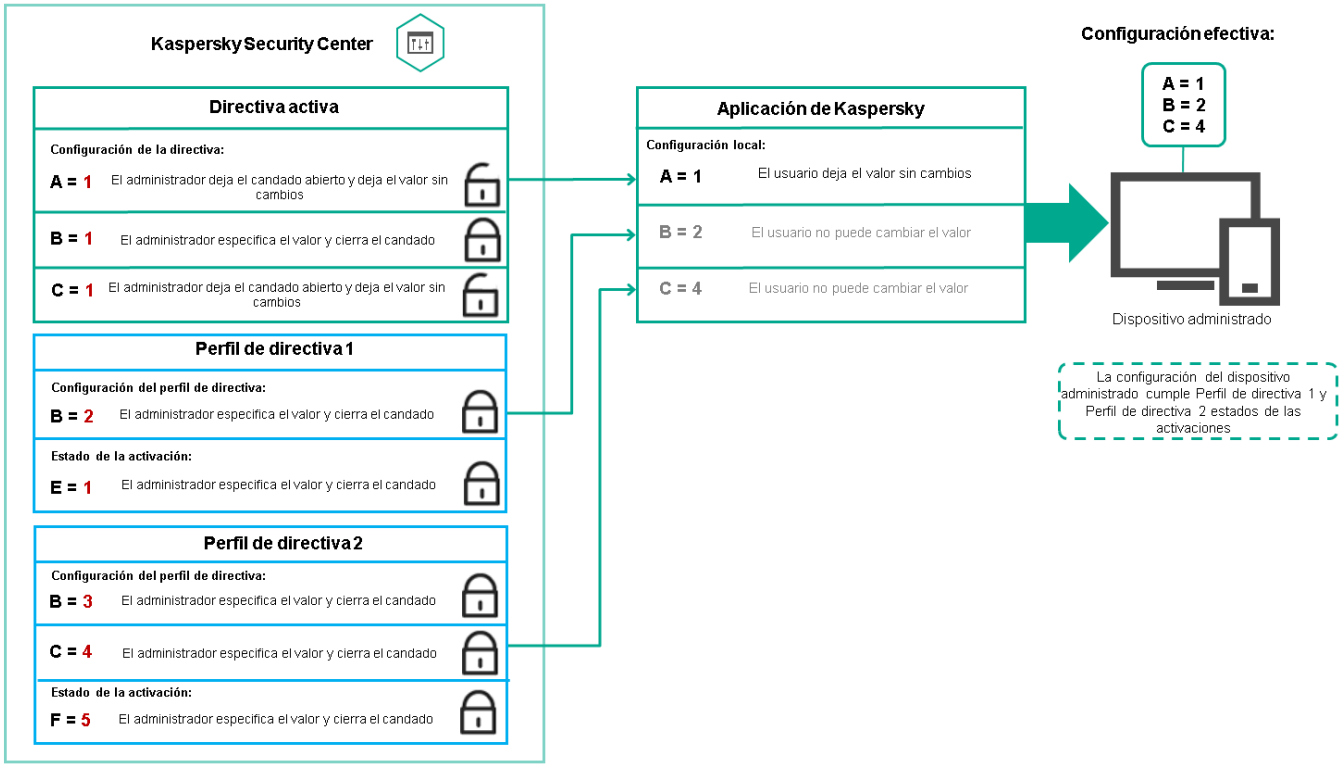
Perfiles de directivas en una jerarquía de directivas

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).



- 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).



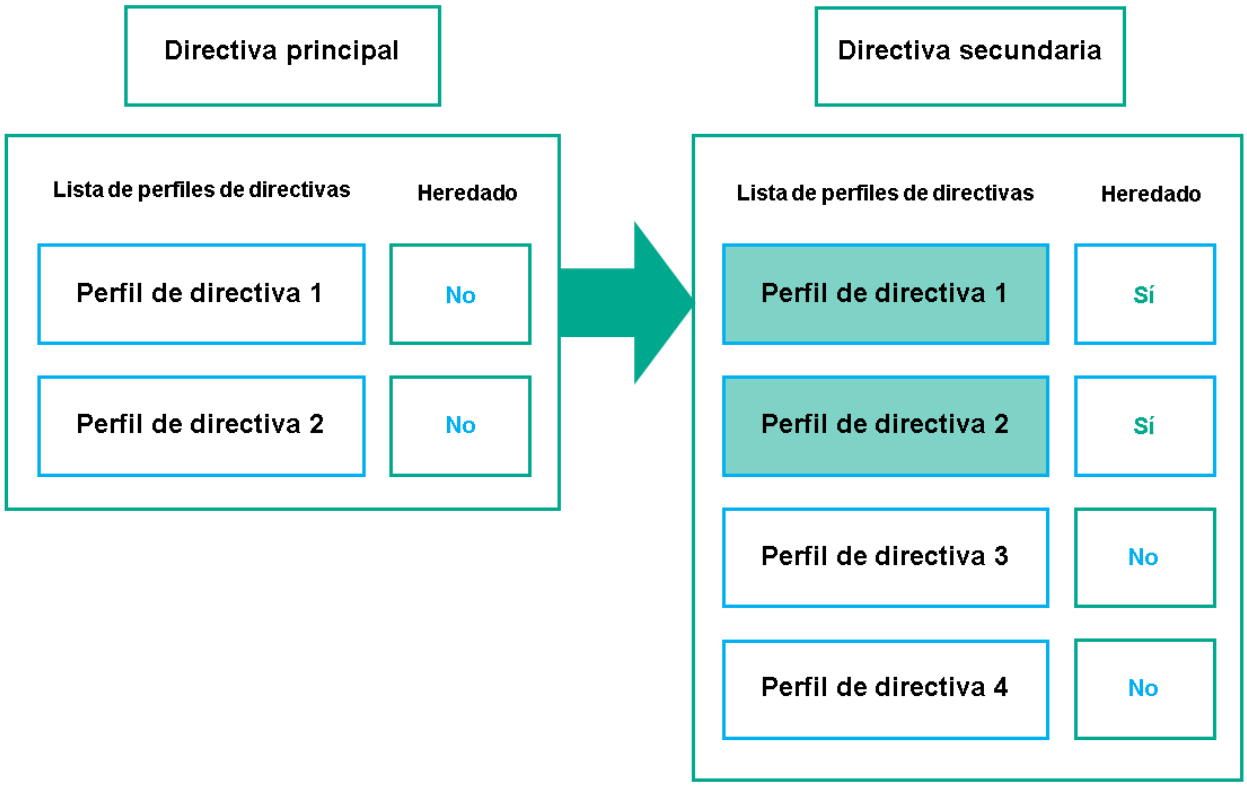
La configuración del dispositivo administrado cumple las condiciones de activación de varios perfiles de directiva

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).

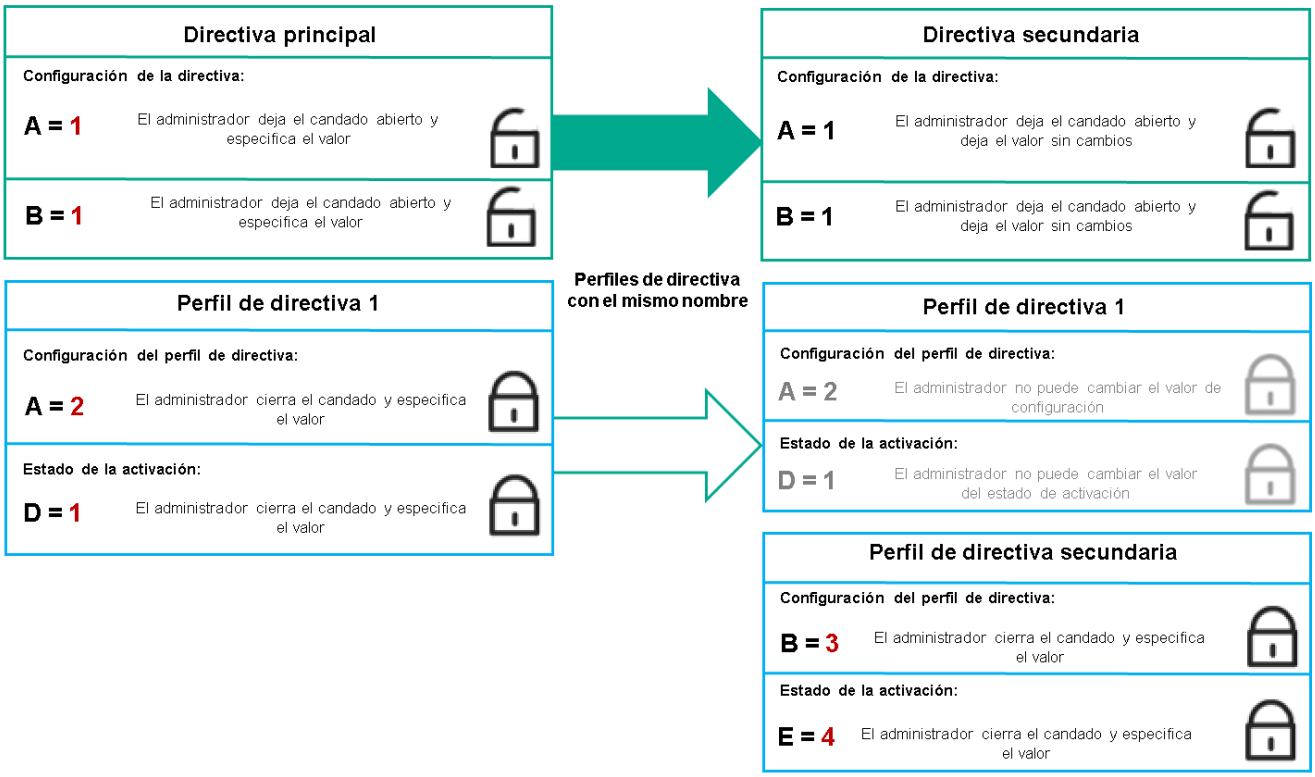


Herencia de perfiles de directivas

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.

> No puede crear una directiva del Servidor de administración.

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. Haga clic en 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).

   La configuración de la aplicación depende de la aplicación para la que crea una directiva. Para más detalles, consulte los siguientes recursos:

- Configuración del Servidor de administración
- Ajustes de la directiva del Agente de red
- Documentación de Kaspersky Endpoint Security para Windows

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.

Modificar una directiva

Para modificar una directiva:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en la directiva que desee modificar.

   Se abre la ventana de configuración de la directiva.
3. Especifique la configuración general y la configuración de la aplicación para la que crea una directiva. Para más detalles, consulte los siguientes recursos:
   - Configuración del Servidor de administración
   - Ajustes de la directiva del Agente de red
   - Documentación de Kaspersky Endpoint Security para Windows

   Si necesita información detallada para configurar otra aplicación de seguridad, consulte la documentación de ese software.
4. Haga clic en **Guardar**.

Los cambios realizados en la directiva se guardarán en las propiedades de la directiva y aparecerán en la sección **Historial de revisión**.

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**
- **Fuera de la oficina**

  Una directiva "fuera de la oficina" entra en vigor (es decir, se activa) cuando el dispositivo sale de la red corporativa.

- **Inactiva**

  Si selecciona esta opción, la directiva estará inactiva, pero quedará guardada en la carpeta **Directivas**. Podrá activarla cuando resulte necesario.

- En el grupo de ajustes **Herencia de configuración**, puede configurar las opciones de directiva:
  - **Heredar configuración de la directiva principal**

    Si habilita esta opción, la directiva heredará los valores de configuración definidos en la directiva del grupo de nivel superior. Estos valores, en consecuencia, estarán bloqueados.

    Esta opción está 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

La pestaña **Configuración de eventos** le permite configurar el registro de eventos y la notificación 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:

  - **Almacenar en la base de datos del Servidor de administración durante (días)**
  - **Almacenar en el registro de eventos del SO del dispositivo**

- **Notificaciones de eventos**

  Puede seleccionar si desea que se le notifique sobre el evento por correo electrónico.

  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 lo desea, puede cambiar esta configuración en la pestaña **Correo electrónico**.

Además, la pestaña **Configuración de eventos** muestra una notificación cuando se añaden nuevos tipos de eventos (por ejemplo, en una nueva versión del producto) y le permite aplicar la nueva configuración haciendo clic en el botón **Guardar** o **Guardar y cerrar**.

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.

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 principal** 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 principal** 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 principal** 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 principal** 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 Cloud Console 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 Cloud Console 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)**.

Ver el gráfico de distribución de una directiva

En Kaspersky Security Center Cloud Console, 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, haga clic en el enlace **Distribución**.

   Se abre la ventana **<Nombre de la directiva>: resultados de la distribución**.
4. En la ventana de **Resultados de distribución de <Nombre de la directiva>** que se abre, se muestra la **Descripción del estado (si está disponible)** de la directiva.

Puede cambiar la cantidad de resultados que aparecen en la lista que detalla la distribución de la directiva. La cantidad máxima de dispositivos es 100 000.

Para cambiar la cantidad de dispositivos que se muestran en la lista con los resultados de la distribución de una directiva:

1. En el menú principal, vaya a la configuración de su cuenta y, a continuación, elija **Opciones de interfaz**.
2. En el **Número máximo de dispositivos que se muestran en los resultados de la distribución de directivas**, introduzca la cantidad de dispositivos (hasta 100 000).

   De manera predeterminada, el límite es de 5000.
3. Haga clic en **Guardar**.

El cambio se aplica y se guarda.

Activar una directiva automáticamente ante un brote de virus

Para que una directiva se active automáticamente al ocurrir un evento Brote de virus, haga lo siguiente:

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.

2. Elija la sección **Brote de virus**.

3. En el panel de la derecha, haga clic en el vínculo **Configurar directivas para activar cuando se produce un evento de brote de virus**.

   Se abre la ventana **Activación de directiva**.

4. En la sección relativa al componente que detecta el brote de virus ("Antivirus para estaciones de trabajo y servidores de archivos", "Antivirus para servidores de correo" o "Antivirus para defensa del perímetro"), busque la entrada que desea, seleccione la opción adyacente a la misma y haga clic en el botón **Añadir**.

   Se abre una ventana con el grupo de administración **Dispositivos administrados**.

5. Haga clic en el ícono (>) ubicado junto a **Dispositivos administrados**.

   Se muestra una jerarquía de grupos de administración y sus directivas.

6. En la jerarquía de grupos de administración y directivas, haga clic en el nombre de la directiva que se activará cuando se detecte un brote de virus. Puede seleccionar más de una directiva.

   Para seleccionar todas las directivas incluidas en el grupo o en la lista, active la casilla ubicada junto al nombre pertinente.

7. Haga clic en el botón **Guardar**.

   Se cierra la ventana con la jerarquía de grupos de administración y directivas.

Las directivas seleccionadas se agregan a la lista de directivas que se activarán cuando se detecte un brote de virus. Estas directivas se activarán independientemente del estado que tengan antes del brote de virus (activa o inactiva).

Si desea reaplicar la directiva que se encontrara en vigor antes del brote de virus, deberá hacer el cambio en forma manual.

Sincronización forzada

Si bien Kaspersky Security Center Cloud Console 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** → **Grupos** y seleccione el grupo de administración que contiene los dispositivos que desea 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 **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, usted 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.

Eliminar una directiva

Puede eliminar una directiva si ya no la necesita. Puede eliminar directivas que el grupo de administración especificado no haya heredado. Una directiva heredada solo se puede eliminar en el grupo de administración de nivel superior para el que fue creada.

Para eliminar una directiva:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Marque la casilla ubicada junto a la directiva que desee eliminar y haga clic en **Eliminar**.

   El botón **Eliminar** no estará disponible (estará atenuado) si se ha seleccionado una directiva heredada.
3. Haga clic en **Aceptar** para confirmar la operación.

La directiva se elimina junto con todos sus perfiles.

Administración de perfiles de directivas

Esta sección trata sobre la administración de perfiles de directivas. Encontrará instrucciones para ver los perfiles de una directiva; cambiar la prioridad de un perfil de directiva; crear, copiar, modificar o eliminar un perfil de directiva, y crear una regla de activación para un perfil de directiva.

Ver los perfiles de una directiva

Para ver los perfiles de una directiva:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el nombre de la directiva cuyos perfiles desee ver.

   Se abre la ventana de propiedades de la directiva, con la pestaña **General** seleccionada.
3. Abra la pestaña **Perfiles de directiva**.

Aparece la lista de perfiles de directiva en formato tabular. Si la directiva no tiene perfiles, verá una tabla vacía.

Cambiar la prioridad de un perfil de directiva

Para cambiar la prioridad de un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.
2. En la pestaña **Perfiles de directiva**, marque la casilla correspondiente al perfil de directiva que cambiará de prioridad.
3. Cambie la posición del perfil de directiva en la lista haciendo clic en los botones **Priorizar** o **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.

Modificar un perfil de directiva

La posibilidad de modificar un perfil de directiva solo está disponible para las directivas de Kaspersky Endpoint Security para Windows.

Para modificar un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.

2. En la pestaña **Perfiles de directiva**, seleccione el perfil de directiva que desee modificar.

   Se abre la ventana de propiedades del perfil de directiva.

3. En la ventana de propiedades, configure el perfil:

   - De ser necesario, en la pestaña **General**, habilite o deshabilite el perfil y cámbiele el nombre.
   - Modifique las reglas de activación del perfil.

- Modifique los ajustes de la aplicación.

Para obtener detalles sobre los ajustes de las aplicaciones de seguridad, consulte la documentación de esas aplicaciones.

4. Haga clic en **Guardar**.

Los cambios de configuración entrarán en vigor cuando el dispositivo se sincronice con el Servidor de administración (si el perfil de directiva está activo) o cuando se accione una de las reglas de activación (si el perfil de directiva está inactivo).

Copiar un perfil de directiva

Puede copiar un perfil de directiva a la directiva actual o a otra si, por ejemplo, quiere tener perfiles idénticos para directivas diferentes. También puede copiar un perfil si necesita tener dos o más perfiles que se diferencien solo en un pequeño número de ajustes.

Para copiar un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva. Si la directiva no tiene perfiles, verá una tabla vacía.

2. En la pestaña **Perfiles de directiva**, seleccione el perfil de directiva que desee copiar.

3. Haga clic en **Copiar**.

4. En la ventana que se abre, seleccione la directiva a la que desee copiar el perfil.

   Puede copiar un perfil de directiva en la misma directiva o en una directiva que especifique.

5. Haga clic en **Copiar**.

El perfil de directiva se copia a la directiva seleccionada. La copia del perfil obtiene la prioridad más baja. Cuando un perfil se copia a su misma directiva de origen, se agrega un índice numérico entre paréntesis al nombre de la copia (por ejemplo: (1), (2), etc.).

Más adelante, podrá cambiar la configuración del perfil, incluyendo su nombre y su prioridad; el perfil de directiva original no sufrirá modificaciones.

Crear una regla de activación para un perfil de directiva

Para crear una regla de activación para un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.

2. En la pestaña **Perfiles de directiva**, haga clic en el perfil de directiva para el que desee crear la regla de activación.

   Si la lista de perfiles de la directiva está vacía, puede crear un perfil de directiva.

3. En la pestaña **Reglas de activación**, haga clic en el botón **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 "≠").

  Tenga en cuenta que la lista de usuarios se filtra y muestra los propietarios de dispositivos que son usuarios internos.

  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 Cloud Console. 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 "≠").

    Tenga en cuenta que la lista de usuarios se filtra y muestra los propietarios de dispositivos que son usuarios internos.

    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 Cloud Console. 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:

  - Etiqueta

    En la lista de etiquetas, configure la regla que hará que los dispositivos que tengan ciertas etiquetas se incluyan en el perfil de directiva. Para configurar esta regla, active las casillas ubicadas junto a las etiquetas pertinentes.

    Si necesita agregar etiquetas nuevas, introdúzcalas en el campo que se encuentra sobre la lista y haga clic en el botón **Agregar**.

    El perfil de directiva incluirá aquellos dispositivos que, en su descripción, contengan todas las etiquetas seleccionadas. Si no activa estas casillas, no se aplicará este criterio. Estas casillas están desactivadas de manera predeterminada.

  - Aplicar a los dispositivos que no tengan 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.

- **Reglas para el uso de Active Directory**

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo si el mismo pertenece a una unidad organizativa de Active Directory en particular o si el dispositivo o su propietario son miembros de un grupo de seguridad de Active Directory.

  Si elige esta opción, defina esto en el paso siguiente:

  - **Membresía del propietario del dispositivo en un grupo de seguridad de Active Directory**

    Si habilita esta opción, el perfil de directiva se activará en un dispositivo si su propietario es miembro del grupo de seguridad especificado. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de manera predeterminada.

  - **Pertenencia del dispositivo al grupo de seguridad de Active Directory**

    Si habilita esta opción, el perfil de directiva se activará en el dispositivo. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de manera predeterminada.

  - **Asignación de dispositivos en la unidad organizativa de Active Directory**

    Si habilita esta opción, el perfil de directiva se activará en un dispositivo si el mismo está incluido en la unidad organizativa de Active Directory especificada. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil.

    Esta opción está deshabilitada de 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.

Protección y cifrado de datos

El cifrado de datos reduce el riesgo de pérdida involuntaria de datos en caso de que le roben o pierda su ordenador portátil o su disco duro, o en caso de que usuarios no autorizados y aplicaciones accedan a ellos.

Las siguientes aplicaciones de Kaspersky son compatibles con el cifrado de datos:

- Kaspersky Endpoint Security para Windows
- Kaspersky Endpoint Security for Mac

Puede modificar los ajustes de la interfaz de usuario para mostrar u ocultar algunos de los elementos de la interfaz que están vinculados a la función de administración del cifrado.

Cifrado de datos en Kaspersky Endpoint Security para Windows

Puede administrar la tecnología de Cifrado de unidad BitLocker en dispositivos que ejecuten un sistema operativo Windows para servidores o estaciones de trabajo.

Al usar estos componentes de Kaspersky Endpoint Security para Windows puede, por ejemplo, activar o desactivar el cifrado, ver la lista de unidades cifradas o generar y ver informes sobre el cifrado.

El cifrado se configura al definir las directivas de Kaspersky Endpoint Security para Windows en Kaspersky Security Center Cloud Console. Kaspersky Endpoint Security para Windows realizará las operaciones de cifrado y descifrado que se indiquen en la directiva activa. Si desea obtener instrucciones detalladas sobre cómo configurar reglas, así como una descripción de las funciones de cifrado, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

Cifrado de datos en Kaspersky Endpoint Security for Mac

En dispositivos con macOS, puede utilizar el cifrado FileVault. Esta tecnología de cifrado puede habilitarse y deshabilitarse a través de Kaspersky Endpoint Security for Mac.

El cifrado se configura al definir las directivas de Kaspersky Endpoint Security for Mac en Kaspersky Security Center Cloud Console. Kaspersky Endpoint Security for Mac realizará las operaciones de cifrado y descifrado que se indiquen la directiva activa. Para obtener información detallada sobre las funciones de cifrado, consulte la Ayuda de Kaspersky Endpoint Security for Mac.

Ver la lista de unidades cifradas

En Kaspersky Security Center Cloud Console 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**.

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. Abra la sección **Dispositivos cifrados** para generar el Informe sobre el estado del cifrado de los dispositivos de almacenamiento masivo o el informe sobre los derechos de acceso a dispositivos cifrados.
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 correspondiente a la aplicación de Kaspersky que se haya utilizado para cifrar la unidad seleccionada.

   > Si una unidad está cifrada con una aplicación de Kaspersky que no es compatible con Kaspersky Security Center Cloud Console, utilice la Consola de administración basada en Microsoft Management Console para conceder el acceso desconectado.
6. Siga las instrucciones proporcionadas en la Ayuda de Kaspersky Endpoint Security para Windows (consulte los bloques de expansión al final de la sección).

Tras hacerlo, el usuario aplica el archivo recibido para acceder a la unidad cifrada y leer los datos almacenados en la unidad.

Usuarios y roles de usuario

En esta sección se explica qué son, cómo se crean y cómo se modifican los usuarios y los roles de usuario. También se brindan instrucciones para asignar roles y grupos a los usuarios y para asociar los roles a perfiles de directivas.

Acerca de las cuentas de usuario

Kaspersky Security Center Cloud Console le permite administrar cuentas de usuario y grupos de cuentas. La aplicación admite tres tipos de cuentas:

- Cuentas de empleados de la organización. El Servidor de administración obtiene los datos de las cuentas de estos usuarios del dominio cuando sondea el controlador de dominio de la organización.
- Cuentas de usuarios locales. Cuentas locales de dispositivos administrados, así como cuentas locales del dispositivo en el que está instalado el Servidor de administración.
- Cuentas de usuarios internos de Kaspersky Security Center Cloud Console. Puede crear cuentas de usuarios internos. Estas cuentas se utilizan solo en Kaspersky Security Center Cloud Console.

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. De forma predeterminada, la tabla abierta se filtra por las columnas **Subtipo** y **Tiene funciones asignadas**. La tabla muestra los usuarios internos o los grupos que tienen roles asignados.

Si desea que la tabla solo muestre las cuentas de usuarios locales, establezca los criterios de filtro de **Subtipo** en **Local**.

Si cambia a un Servidor de administración secundario versión 14.2 o anterior y luego abre la lista de usuarios o grupos de seguridad, la tabla abierta se filtrará solo por la columna **Subtipo**. El filtro de la columna **Tiene funciones asignadas** no se aplica de forma predeterminada. La tabla filtrada contiene todos los usuarios internos o grupos de seguridad con la función asignada y sin ella.

Agregar una cuenta de un usuario interno

Si lo desea, puede añadir usuarios internos de su espacio de trabajo en el portal. Tras añadir un usuario interno, puede asignarle una función en Kaspersky Security Center Cloud Console.

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 Cloud Console proporciona recursos para el acceso basado en roles a las funciones de Kaspersky Security Center Cloud Console 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 Cloud Console 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 Cloud Console con los derechos de acceso para administrar las tareas, los informes y la configuración 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**.

Las **Características generales**: **el área funcional de acceso a los objetos, independientemente de sus listas de control de acceso**, está destinada a fines de auditoría. Cuando los usuarios reciben derechos de **lectura** en esta área funcional, obtienen acceso de **lectura** completo a todos los objetos y pueden ejecutar cualquier tarea creada en elecciones de dispositivos conectados al Servidor de administración a través del Agente de red con derechos de administrador local (raíz para Linux). Recomendamos conceder estos derechos con precaución y a un conjunto limitado de usuarios que los necesiten para realizar sus funciones oficiales.

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: derecho necesario para realizar la acción	Tarea	Informe	Otro
Características generales: **Administración de grupos de administración**	**Escritura**	• Añadir dispositivos a un grupo de administración: **Escritura** • Eliminar dispositivos de un grupo de administración: **Escritura** • Agregar un grupo de administración a otro grupo de administración: **Escritura** • Eliminar un grupo de administración de otro grupo de administración: **Escritura**	Ninguno	N/C	N/C
Características generales: **Acceder a**	**Leer**	Obtener acceso de lectura a todos los objetos: **Leer**	Ninguno	N/C	El acceso se concede independientemente

objetos sin importar sus ACL					de otros derechos, incluso si prohíben el acceso de lectura a objetos específicos.
Características generales: **Funcionalidad básica**	• **Leer** • **Escritura** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	• Reglas de movimiento de dispositivos (crear, modificar o eliminar) para el Servidor virtual: **Escritura**, **realizar operaciones en selecciones de dispositivos** • Obtener certificado personalizado del protocolo móvil (LWNGT): **Lectura** • Establecer certificado personalizado del protocolo móvil (LWNGT): **Escritura** • 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 de eventos de Kaspersky: **Leer**	• "Descargar actualizaciones en el repositorio del Servidor de administración" • "Entregar informes" • "Distribuir paquete de instalación" • "Instalar aplicación en Servidores de administración secundarios de forma remota"	• "Informe del estado de la protección" • "Informe de amenazas" • "Informe de los dispositivos más infectados" • "Informe sobre el estado de las bases de datos antivirus" • "Informe de errores" • "Informe de ataques de red" • "Informe conciso sobre las aplicaciones instaladas para la protección de sistemas de correo" • "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 acerca de problemas de seguridad" • "Informe de eventos" • "Informe de actividad de puntos de distribución" • "Informe sobre los Servidores de administración secundarios" • "Informe sobre los eventos de Control de dispositivos"	Ninguno

				• "Informe de vulnerabilidades" • "Informe sobre aplicaciones prohibidas" • "Informe de Control web" • "Informe sobre el estado de cifrado de los dispositivos administrados" • "Informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo" • "Informe sobre los errores de cifrado de archivos" • "Informe sobre el bloqueo de acceso a los archivos cifrados" • "Informe sobre derechos de acceso a los dispositivos cifrados" • "Informe sobre permisos de usuario vigentes" • "Informe sobre derechos"	
Características generales: **Objetos eliminados**	• **Leer** • **Escritura**	• Ver objetos eliminados en la Papelera de reciclaje: **Leer** • Eliminar objetos de la Papelera de reciclaje: **Escritura**	Ninguno	N/C	N/C
Características generales: **Procesamiento de eventos**	• **Eliminar eventos** • **Editar la configuración de notificaciones sobre los eventos** • **Editar la configuración del registro de eventos** • **Escritura**	• Cambiar los ajustes de registro de eventos: **Editar la configuración de registro de eventos** • Cambiar los ajustes de las notificaciones sobre los eventos: **Editar configuración de notificación de eventos** • Eliminar eventos: **Eliminar eventos**	Ninguno	N/C	Configuración: • Configuración de brotes de virus: número de detecciones de virus necesarias para crear un evento de brote de virus • Configuración de brotes de virus: período sobre el que se evalúan las detecciones de virus

					• Cantidad máxima de eventos almacenados en la base de datos • Período por el que se almacenan los eventos de los dispositivos eliminados
Características generales: **Despliegue del software de Kaspersky**	• **Administrar parches de Kaspersky** • **Leer** • **Escritura** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	Aprobar o rechazar la instalación del parche: **Administrar parches de Kaspersky**	Ninguno	• "Informe sobre el uso de claves de licencia por Servidor de administración virtual" • "Informe de versiones del software de Kaspersky" • "Informe de aplicaciones incompatibles" • "Informe sobre la versión de las actualizaciones para los módulos de software de Kaspersky" • "Informe del despliegue de la protección"	Paquete de instalación: "Kaspersky"
Funciones generales: **administración de claves de licencia**	• **Exportar archivo de clave** • **Escritura**	• Exportar un archivo de clave: **Exportar archivo de clave** • Modificar la configuración de la clave de licencia del Servidor de administración: **Escritura**	Ninguno	N/C	N/C
Características generales: **Administración de informes**	• **Leer** • **Escritura**	• Crear informes independientemente de sus ACL: **Escribir** • Ejecutar informes independientemente de sus ACL: **Leer**	Ninguno	N/C	N/C
Características generales: **Jerarquía de Servidores de administración**	**Configurar los parámetros de jerarquía del Servidor de administración**	Registrar, actualizar o eliminar Servidores de administración secundarios: **Configurar la jerarquía de Servidores de administración**	Ninguno	N/C	N/C
Características generales: **Permisos de usuario**	**Modificar ACL de objeto**	• Cambiar las propiedades de seguridad de cualquier objeto: **Modificar ACL de objeto**	Ninguno	N/C	N/C

		• Administrar roles de usuario: **Modificar ACL de objeto** • Administrar usuarios internos: **Modificar ACL de objeto** • Administrar grupos de seguridad: **Modificar ACL de objeto** • Administrar alias: **Modificar ACL de objeto**			
Características generales: **Servidores de administración virtuales**	• **Administración de Servidores de administración virtuales** • **Leer** • **Escritura** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	• Obtener la lista de Servidores de administración virtuales: **Leer** • Obtener información sobre el Servidor de administración virtual: **Leer** • Crear, actualizar o eliminar un Servidor de administración virtual: **Administrar Servidores de administración virtuales** • Mover un Servidor de administración virtual a otro grupo: **Administrar Servidores de administración virtuales** • Definir los permisos de un Servidor de administración virtual: **Administrar Servidores de administración virtuales**	Ninguno	"Informe sobre los resultados de la instalación de actualizaciones de software de terceros"	Ninguno
Características generales: Administración de claves de cifrado	**Escritura**	Importar las claves de cifrado: **Escritura**	Ninguno	N/C	N/C
Administración de sistemas: **Conectividad**	• **Iniciar sesiones RDP** • **Conexión a sesiones de RDP existentes** • **Iniciar la tunelización** • **Guardar los archivos de los dispositivos en la estación de trabajo del administrador**	• Crear una sesión de escritorio compartido: **Derecho para crear una sesión de escritorio compartido** • Crear una sesión de RDP: **Conexión a sesiones de RDP existentes** • Crear un túnel: **Iniciar la tunelización** • Guardar la lista de red de contenido: **Guardar archivos de los dispositivos en la**	Ninguno	"Informe sobre los usuarios de los dispositivos"	Ninguno

	• **Leer** • **Escritura** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	**estación de trabajo del administrador**			
Administración de sistemas: **Inventario de hardware**	• **Leer** • **Escritura** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	• Obtener o exportar un objeto del inventario de hardware: **Leer** • Agregar, definir o eliminar un objeto del inventario de hardware: **Escribir**	Ninguno	• "Informe sobre el registro de hardware" • "Informe sobre los cambios en la configuración" • "Informe de hardware"	Ninguno
Administración de sistemas: **Control de acceso a la red**	• **Leer** • **Escritura**	• Ver la configuración de CISCO: **Leer** • Cambiar la configuración de CISCO: **Escribir**	Ninguno	N/C	N/C
Administración de sistemas: **Despliegue de sistemas operativos**	• **Desplegar servidores PXE** • **Leer** • **Escritura** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	• Desplegar servidores PXE: **Desplegar servidores PXE** • Ver una lista de servidores PXE: **Leer** • Iniciar o detener el proceso de instalación en clientes PXE: **Ejecutar** • Administrar controladores para WinPE y las imágenes del sistema operativo: **Escritura**	"Crear un paquete de instalación con la imagen del SO de un dispositivo de referencia"	Ninguno	Paquete de instalación: "Imagen del SO"
Administración de sistemas: **Administración de vulnerabilidades y parches**	• **Leer** • **Escritura** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	• Ver propiedades de parches de terceros: **Leer** • Cambiar las propiedades del parche de terceros: **Escritura**	• "Sincronización con Windows Update" • "Instalar actualizaciones de Windows Update" • "Reparar vulnerabilidades" • "Instalar actualizaciones requeridas y reparar vulnerabilidades"	"Informe de actualizaciones de software"	Ninguno
Administración de sistemas: **Instalación remota**	• **Leer** • **Escritura**	• Consulte las propiedades del paquete de instalación basado en Administración de	Ninguno	N/C	Paquetes de instalación: • "Aplicación personalizada"

	• **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	vulnerabilidades y parches de terceros: **Leer** • Cambiar las propiedades del paquete de instalación basado en Administración de vulnerabilidades y parches de terceros: **Escritura**			• "Paquete VAPM"
Administración de sistemas: **Inventario de software**	• **Leer** • **Escritura** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	Ninguno	N/C	• "Informe sobre aplicaciones instaladas" • "Informe del historial del registro de aplicaciones" • "Informe sobre el estado de los grupos de aplicaciones con licencia" • "Informe sobre claves de licencia de software de terceros"	Ninguno

Roles de usuario predefinidos

Las funciones de usuario asignadas a los usuarios de Kaspersky Security Center Cloud Console 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 Cloud Console se pueden asociar con puestos de trabajo específicos, por ejemplo, **Auditor**, **Director de seguridad** y **Supervisor** (estas funciones están presentes en Kaspersky Security Center Cloud Console a partir de la versión 11). Los derechos de acceso de estos roles están preconfigurados para facilitar las obligaciones y las tareas típicas de los puestos asociados. En la siguiente tabla, se muestra cómo estos roles pueden vincularse a puestos de trabajo específicos.

Ejemplos de roles para puestos de trabajo específicos

Rol	Comentario
Auditor	Permite 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 **Leer** y **Escribir** en el área **Objetos eliminados**). 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 **Administración de sistemas**: **Conectividad**. Puede asignar este rol al responsable de la seguridad de TI de su organización.

En la siguiente tabla, se muestran los derechos de acceso asignados a cada rol de usuario predefinido.

Derechos de acceso de los roles de usuario predefinidos

Rol	Descripción

Administrador del Servidor de administración	Permite todas las operaciones en las siguientes áreas funcionales:
	• **Características generales**:
	  • **Funcionalidad básica**
	  • **Procesamiento de eventos**
	  • **Jerarquía de Servidores de administración**
	  • **Servidores de administración virtuales**
	• **Administración de sistemas**:
	  • **Conectividad**
	  • **Inventario de hardware**
	  • **Inventario de software**
	Otorga los derechos de **lectura** y **escritura** en el área funcional **Características generales: Administración de claves de cifrado**.

Operador del Servidor de administración	Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales:
	• **Características generales**:
	  • **Funcionalidad básica**
	  • **Servidores de administración virtuales**
	• **Administración de sistemas**:
	  • **Conectividad**
	  • **Inventario de hardware**
	  • **Inventario de software**

Auditor	Permite todas las operaciones en las siguientes áreas funcionales, en **Características generales**: • **Acceder a objetos sin importar sus ACL** • **Objetos eliminados** • **Administración de informes forzados** Puede asignar este rol a la persona que realiza la auditoría de su organización.

Administrador de instalación	Permite todas las operaciones en las siguientes áreas funcionales:
	• **Características generales**:
	  • **Funcionalidad básica**
	  • **Despliegue del software de Kaspersky**
	  • **Administración de claves de licencia**
	• **Administración de sistemas**:
	  • **Despliegue del sistema operativo**
	  • **Administración de vulnerabilidades y parches**
	  • **Instalación remota**
	  • **Inventario de software**

	Otorga derechos de **lectura** y **ejecución** en el área funcional **Características Generales: Servidores de administración Virtual**.

Operador de instalación	Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales:
	• **Características generales**:
	  • **Funcionalidad básica**
	  • **Despliegue del software de Kaspersky** (también otorga el derecho **Administrar parches de Kaspersky** en esta área)
	  • **Servidores de administración virtuales**
	• **Administración de sistemas**:
	  • **Despliegue del sistema operativo**
	  • **Administración de vulnerabilidades y parches**
	  • **Instalación remota**
	  • **Inventario de software**

Administrador de Kaspersky Endpoint Security	Permite todas las operaciones en las siguientes áreas funcionales: • **Características generales: funcionalidad básica** • Área de Kaspersky Endpoint Security (se incluyen todas las funciones) Otorga los derechos de **lectura** y **escritura** en el área funcional **Características generales: Administración de claves de cifrado**.
Operador de Kaspersky Endpoint Security	Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales: • **Características generales: funcionalidad básica** • Área de Kaspersky Endpoint Security (se incluyen todas las funciones)
Administrador principal	Permite todas las operaciones en áreas funcionales, *excepto* en las siguientes áreas, en **Funciones generales**: • **Acceder a objetos sin importar sus ACL** • **Administración de informes forzados** Otorga los derechos de **lectura** y **escritura** en el área funcional **Características generales: Administración de claves de cifrado**.

Operador principal	Otorga los derechos **Leer** y **Ejecutar** (cuando corresponde) en las siguientes áreas funcionales:
	• **Características generales**:
	  • **Funcionalidad básica**
	  • **Objetos eliminados**
	  • **Operaciones en el Servidor de administración**
	  • **Implementación de la aplicación de Kaspersky**
	  • **Servidores de administración virtuales**
	• **Administración de dispositivos móviles: General**
	• **Administración de sistemas** (se incluyen todas las funciones)
	• Área de Kaspersky Endpoint Security (se incluyen todas las funciones)

Administrador de Administración de dispositivos móviles	Permite todas las operaciones en las siguientes áreas funcionales: • **Características generales: funcionalidad básica** • **Administración de dispositivos móviles: General**
Operador de	Otorga los derechos **Leer** y **Ejecutar** en el área funcional **Características generales**: **Funcionalidad básica**.

Administración de dispositivos móviles	Otorga los derechos **Leer** y **Enviar únicamente comandos de información a dispositivos móviles** en **Administración de dispositivos móviles**: **General** área funcional:
Director de seguridad	Permite todas las operaciones en las siguientes áreas funcionales, en **Características generales**: • **Acceder a objetos sin importar sus ACL** • **Administración de informes forzados** Otorga derechos de **Lectura**, **Escritura**, **Ejecución**, **Guardar archivos desde los dispositivos a la estación de trabajo del administrador** y **Realizar operaciones para las selecciones de dispositivos** en el área funcional **Administración del sistema: Conectividad**. Puede asignar este rol al responsable de la seguridad de TI de su organización.
Analista senior de seguridad	Otorga el derecho de **lectura** en el área funcional **Funciones generales**: **Funcionalidad básica**. Otorga derechos de **Lectura**, **Escritura**, **Ejecución**, **Guardar archivos desde los dispositivos a la estación de trabajo del administrador** y **Realizar operaciones para las selecciones de dispositivos en el área funcional Administración del sistema**: **Conectividad**. Otorga los derechos de acceso a la solución Kaspersky Endpoint Detection and Response Expert.
Usuario de Self Service Portal	Permite todas las operaciones en el área funcional **Administración de dispositivos móviles: Self Service Portal**. Esta función no es compatible con Kaspersky Security Center 11 ni versiones posteriores.
Supervisor	Otorga el derecho de **lectura** en las áreas funcionales **Funciones generales**: **Acceder a objetos, independientemente de sus ACL** y **Funciones generales**: **Gestión reforzada de informes**. Puede asignar este rol a un Director de seguridad y a otras personas que tengan a su cargo la seguridad de TI de la organización.
Administrador de Administración de vulnerabilidades y parches	Permite todas las operaciones en las áreas funcionales **Características generales**: **Funcionalidad básica** y **Administración de sistemas** (se incluyen todas las funciones).
Operador de Administración de vulnerabilidades y parches	Otorga los derechos **Leer** y **Ejecutar** (cuando corresponde) en las áreas funcionales **Características generales**: **Funcionalidad básica** y **Administración de sistemas** (se incluyen todas las funciones).

Asignación de derechos de acceso a objetos específicos

Además de asignar derechos de acceso al nivel de servidor, puede configurar el acceso a objetos específicos, por ejemplo, a una tarea específica. La aplicación le permite especificar derechos de acceso a los siguientes tipos de objetos:

- Grupos de administración
- Tareas
- Informes
- Selecciones de dispositivos
- Selecciones de eventos

Para asignar derechos de acceso a un objeto específico:

1. Según el tipo de objeto, en el menú principal vaya a la sección correspondiente:
   - **Activos (dispositivos) → Jerarquía de grupos**
   - **Activos (dispositivos) → Tareas**
   - **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 de seguridad

Puede otorgar derechos de acceso a usuarios y grupos de seguridad para que usen diferentes funciones del Servidor de administración, por ejemplo, Kaspersky Endpoint Security for Linux.

Para asignar derechos de acceso a un usuario o grupo de seguridad, haga lo siguiente:

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Derechos de acceso**, 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:

- Funciones generales:
  - Administración de grupos de administración
  - Acceder a objetos independientemente de sus ACL
  - Funcionalidad básica
  - Objetos eliminados
  - Administración de claves de cifrado
  - Procesamiento de eventos
  - Operaciones en el Servidor de administración (solo en la ventana de propiedades del Servidor de administración)
  - Etiquetas de dispositivos
  - Implementación de la aplicación de Kaspersky
  - Administración de claves de licencia
  - Integración de la aplicación
  - Administración de informes aplicada
  - Jerarquía de Servidores de administración
  - Permisos de usuario
  - Servidores de administración virtual
- Administración de dispositivos móviles:
  - General
  - Self Service Portal
- Administración del sistema:

- Conectividad
- Ejecutar scripts de forma remota
- Inventario de hardware
- Control de acceso a la red
- Despliegue del sistema operativo
- Administración de vulnerabilidades y parches
- 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.

También puede añadir usuarios y grupos de seguridad a la cobertura de una función de usuario para usar diferentes funciones del Servidor de administración. La configuración asociada a una función de usuario se aplica únicamente a los dispositivos que pertenecen a los usuarios que tienen esa función, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados a la función en cuestión.

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**.

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 añadir usuarios, grupos de usuarios 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. Seleccione las casillas de verificación junto a los usuarios o grupos de usuarios que desea añadir al alcance del rol 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 el paso **Seleccionar función**, seleccione el rol de usuario que desee asignar.

5. En el paso **Definir cobertura**, seleccione el grupo de administración que desee añadir al alcance del rol de usuario.

6. Haga clic en el botón **Asignar función** para cerrar la ventana.

Los usuarios o grupos de usuarios seleccionados y el grupo de administración seleccionado se añaden 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 el paso **Definir cobertura**, seleccione el grupo de administración que desee añadir al alcance del rol de usuario.

6. En el paso **Seleccionar usuarios**, seleccione los usuarios y los grupos de seguridad que desee agregar al alcance del rol de usuario.

7. Haga clic en el botón **Asignar función** para cerrar la ventana.

8. Cierre la ventana de propiedades del rol.

Los usuarios o grupos de usuarios seleccionados y el grupo de administración seleccionado se añaden al alcance del rol de usuario.

Método 3:

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Derechos de acceso**, elija la casilla ubicada junto al nombre del usuario o el grupo de seguridad que desea añadir a la cobertura de una función de usuario y, a continuación, haga clic en el botón **Funciones**.

   No puede elegir varios usuarios o grupos de seguridad al mismo tiempo. Si selecciona más de un elemento, el botón **Funciones** se desactivará.

3. En la ventana **Funciones**, seleccione la función de usuario que desea asignar, haga clic en **Aceptar** y guarde los cambios.

   Los usuarios o grupos de seguridad seleccionados se añaden a la cobertura de la función 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.

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 **Grupo nuevo**.
3. En la ventana **Grupo nuevo**, especifique la siguiente configuración para el nuevo grupo de seguridad:

- **Nombre**
- **Descripción**

4. Haga clic en **Correcto** para guardar los cambios.

Se añade un nuevo grupo de seguridad a la lista de grupos de seguridad.

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.

Agregar cuentas de usuario a un grupo interno

Las únicas cuentas que se pueden agregar a un grupo interno son las de usuarios internos.

Para agregar cuentas de usuario a un grupo interno:

1. En el menú principal, vaya a **Usuarios y funciones** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Active las casillas de verificación ubicadas junto a las cuentas de usuario que desee agregar al grupo.
3. Haga clic en el botón **Asignar grupo**.
4. En la ventana **Asignar grupo** que se abre, seleccione el grupo al que desee agregar las cuentas de usuario.
5. Haga clic en el botón **Asignar**.

Las cuentas de usuario se agregan al grupo. También puede añadir usuarios internos a un grupo mediante la configuración del grupo.

Eliminar un grupo de seguridad

Solo se pueden eliminar los grupos de seguridad internos.

Para eliminar un grupo de usuarios, haga lo siguiente:

1. En el menú principal, vaya a **Usuarios y funciones** → **Usuarios y grupos** y luego seleccione la pestaña **Grupos**.
2. Seleccione la casilla de verificación junto al grupo de usuarios que desea eliminar.
3. Haga clic en **Eliminar** y luego confirme la eliminación en la ventana abierta.

   Se elimina el grupo de usuarios.

Configuración de la integración de ADFS

Para permitir que los usuarios registrados en Active Directory (AD) de su organización inicien sesión en Kaspersky Security Center Cloud Console, es necesario configurar la integración con los Servicios de federación de Active Directory (AD FS).

Kaspersky Security Center Cloud Console es compatible con AD FS 3 (Windows Server 2016) o versiones posteriores. AD FS debe estar publicado y disponible en Internet. Como certificado de comunicación de servicio, AD FS utiliza un certificado de confianza público.

Para cambiar la configuración de integración de AD FS, debe tener derechos de acceso para cambiar los permisos de usuario.

Antes de continuar, asegúrese de haber completado el Sondeo de Active Directory.

Para configurar la integración de AD FS:

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**, seleccione la sección **Configuración de integración con ADFS**.
3. Copie la URL de devolución de llamada.

   Necesitará esta URL para configurar la integración en la Consola de administración de AD FS.
4. En la consola de administración de AD FS, añada un nuevo grupo de aplicaciones y, a continuación, añada una nueva aplicación seleccionando la plantilla **Server application** (los nombres de los elementos de interfaz de Microsoft están en inglés).

   La Consola de administración de AD FS genera el ID de cliente para la nueva aplicación. Necesitará el ID de cliente para configurar la integración en Kaspersky Security Center Cloud Console.

5. Como URI de redireccionamiento, especifique la URL de devolución de llamada que copió en la ventana de propiedades del Servidor de administración.

6. Genere una clave secreta de cliente. Necesitará la clave secreta del cliente para configurar la integración en Kaspersky Security Center Cloud Console.

7. Guarde las propiedades de la aplicación añadida.

8. Añada una nueva aplicación al grupo de aplicaciones creado. Esta vez seleccione la plantilla de **API web**.

9. En la pestaña **Identificadores**, en la lista **Identificadores de la parte que confía**, añada el ID de cliente de la aplicación de servidor que añadió anteriormente.

10. En la pestaña **Permisos del cliente**, en la lista **Ámbitos permitidos**, seleccione los ámbitos **allatclaims** y **openid**.

11. En la pestaña **Reglas de transformación de emisiones**, seleccione la plantilla **Enviar atributos LDAP como reclamos** para añadir una nueva regla:

    a. Nombre la regla. Por ejemplo, puede nombrarle 'Group SID'.

    b. Seleccione **Active Directory** como almacén de atributos y luego asigne **Grupos de tokens como SID** como un atributo LDAP a 'Group SID' como un tipo de notificación saliente.

12. En la pestaña **Reglas de transformación de emisiones**, seleccione la plantilla **Enviar reclamaciones mediante una regla personalizada** para añadir una nueva regla:

    a. Nombre la regla. Por ejemplo, puede nombrarle 'ActiveDirectoryUserSID'.

    b. En el campo **Regla personalizada**, escriba:

    ```
    c:[Type ==
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
    Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
    ("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"), query =
    ";objectSID;{0}", param = c.Value);
    ```

13. En Kaspersky Security Center Cloud Console, abra nuevamente la sección **Configuración de integración con ADFS**.

14. Cambie el botón de alternancia a la posición **Integración con ADFS Activada**.

15. Haga clic en el enlace **Configuración** y, a continuación, especifique el archivo que contiene el certificado o varios certificados para el servidor de federación.

16. Haga clic en el enlace **Configuración de integración con ADFS** y, a continuación, especifique la siguiente configuración:

    - **URL del emisor**

      La dirección URL del servidor de federación que se ejecuta en su organización.

      En particular, Kaspersky Security Center Cloud Console añade '/.well-known/openid-configuration' a la dirección URL del emisor e intenta abrir la dirección URL resultante (issuer_URL/.well-known/openid-configuration) para descubrir la configuración del emisor automáticamente.

    - **Id. del cliente**

ID de cliente que genera el servidor de federación para identificar Kaspersky Security Center Cloud Console. Puede encontrar el ID de cliente en la Consola de administración de AD FS en la ventana de propiedades de la aplicación del servidor que corresponde a Kaspersky Security Center Cloud Console.

- **Secreto del cliente**

  Usted genera un secreto de cliente en la Consola de administración de AD FS cuando especifica las propiedades de la aplicación del servidor que corresponde a Kaspersky Security Center Cloud Console.

- **Dominio desde el cual autenticar a los usuarios**

  Los miembros del dominio que seleccione podrán usar sus credenciales de cuenta de dominio para iniciar sesión en Kaspersky Security Center Cloud Console. Los nombres de dominio aparecen en la lista después de completar el sondeo de la red.

- **Nombre de campo para el SID del usuario en el token de ID**

  Nombre del campo que hace referencia al SID del usuario en el token de ID. El nombre del campo es obligatorio para identificar al usuario en Kaspersky Security Center Cloud Console. De forma predeterminada, este campo en el token de ID se denomina 'primarysid'.

- **Nombre de campo para un conjunto de SID de grupos del usuario en el token de ID**

  Nombre del campo que hace referencia a la matriz de SID de los grupos de seguridad de Active Directory en los que está incluido el usuario. De forma predeterminada, este campo en el token de ID se llama 'groupsid'.

17. Haga clic en el botón **Guardar**.

    Se completó la integración con AD FS. Para iniciar sesión en Kaspersky Security Center Cloud Console con las credenciales de una cuenta de AD, utilice el enlace que se proporciona en la sección **Configuración de integración con ADFS** (**Enlace de inicio de sesión a Kaspersky Security Center Cloud Console con ADFS**).

Cuando inicia sesión en Kaspersky Security Center Cloud Console a través de AD FS por primera vez, es posible que la consola responda con retraso.

Configuración de la integración con Microsoft Entra ID

Debe configurar la integración con Microsoft Entra ID para permitir a los usuarios de su organización iniciar sesión en Kaspersky Security Center Cloud Console con sus credenciales de cuenta de Microsoft Entra ID.

La integración con Microsoft Entra ID está disponible solo para el Servidor de administración principal. No puede configurar la integración para Servidores de administración secundarios o virtuales.

Para configurar la integración con Microsoft Entra ID, siga estos pasos:

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 **Microsoft Entra ID**.

3. Active el botón **Integración con Microsoft Entra ID**.

4. Copie los enlaces de los siguientes campos:

   - **URL de devolución de llamada**
   - **URL de cierre de sesión del canal frontal**

     Necesita estas URL para registrar Kaspersky Security Center Cloud Console en el inquilino de Microsoft Entra ID.
   - **URL de inicio de sesión**

     Necesita esta URL para permitir a los usuarios iniciar sesión en el espacio de trabajo de Kaspersky Security Center Cloud Console con sus credenciales de Microsoft Entra ID después de que se complete la integración con Microsoft Entra ID.

5. Inicie sesión en el centro de administración de Microsoft Entra y, a continuación, elija el inquilino de su organización.

   Debe tener la función de administrador global o de administrador de la aplicación en el inquilino.

6. En el menú principal, vaya a **Identidad** → **Aplicaciones** → **Registros de aplicaciones** y, a continuación, haga clic en el botón **Nuevo registro**.

7. En la ventana que se abre, realice una de las siguientes acciones:

   - Especifique un nombre para la aplicación Kaspersky Security Center Cloud Console.
   - En la sección **Tipos de cuenta admitidos**, elija la opción **Solo las cuentas en este directorio organizativo (solo <tenant_name> - Inquilino único)**.
   - En la sección **URI de redireccionamiento**, elija **Web** de la lista desplegable y, a continuación, introduzca la URL de devolución de llamada que copió de Kaspersky Security Center Cloud Console en el paso 4.

8. Haga clic en el botón **Registrar**.

   La aplicación Kaspersky Security Center Cloud Console se registra en Microsoft Entra ID y se abre la página de descripción general de la aplicación.

9. Si es necesario, añada Kaspersky Security Center Cloud Console a la lista de aplicaciones.

   Para abrir Kaspersky Security Center Cloud Console, los usuarios podrán hacer clic en el nombre de la aplicación en la lista en Mis apps y el iniciador de Office 365 sin utilizar la URL de inicio de sesión.

10. Copie el **ID (del cliente) de la aplicación** y el **ID (del inquilino) del directorio** y guárdelos de la forma más conveniente.

    Necesita estos ID al completar los campos obligatorios en Kaspersky Security Center Cloud Console en el paso 14.

11. En el menú de la aplicación Kaspersky Security Center Cloud Console, vaya a la sección **Autenticación** y, a continuación, introduzca las URL que copió de Kaspersky Security Center Cloud Console en el paso 4:

    - En la sección **Web**, haga clic en el botón **Añadir URI** y, a continuación, introduzca la URL de inicio de sesión.
    - En la sección **URL de cierre de sesión del canal frontal**, introduzca la URL de cierre de sesión del canal frontal.

12. En el menú de la aplicación Kaspersky Security Center Cloud Console, vaya a la sección **Certificados y secretos** y, a continuación, siga estos pasos:

    a. Vaya a la pestaña **Secretos del cliente** y haga clic en el botón **Nuevo secreto de cliente**.

    b. En la ventana que se abre, especifique cualquier descripción para el secreto del cliente y, a continuación, elija el período después del cual caduca el secreto.

    Le recomendamos que copie la fecha después de la cual caduca el secreto, de la forma que le parezca más conveniente, para rotar los secretos de manera oportuna.

    a. Haga clic en el botón **Agregar**.

    El secreto creado se muestra en la pestaña **Secretos del cliente**.

    b. Copie la información de la columna **Valor**.

    Le recomendamos que copie la información inmediatamente después de crear el secreto del cliente.

13. En el menú de la aplicación Kaspersky Security Center Cloud Console, vaya a la sección **Configuración del token** y, a continuación, siga estos pasos:

    - Añada el reclamo opcional **onprem_sid**:

        a. Haga clic en el botón **Añadir reclamo opcional**.

        b. En la ventana que se abre, elija el tipo de token **ID** y, a continuación, en la columna **Reclamo**, marque la casilla de verificación ubicada junto a **onprem_sid**.

        c. Haga clic en el botón **Agregar**.

        El reclamo opcional **onprem_sid** aparece en la página **Reclamos opcionales**.

    - Añada el reclamo opcional **preferred_username**:

        a. Haga clic en el botón **Añadir reclamo opcional**.

        b. En la ventana que se abre, elija el tipo de token **Acceso** y, a continuación, en la columna **Reclamo**, marque la casilla de verificación ubicada junto a **preferred_username**.

        c. Haga clic en el botón **Agregar**.

        El reclamo opcional **preferred_username** aparece en la página **Reclamos opcionales**.

14. En el menú de la aplicación Kaspersky Security Center Cloud Console, vaya a la sección **Permisos de la API** y, a continuación, añada los siguientes permisos:

- **User.Read.All**
- **User.Export.All**
- **GroupMember.Read.All**
- **Directory.Read.All**

Para añadir un permiso, siga estos pasos:

a. Haga clic en el botón **Añadir un permiso** y, a continuación, elija la pestaña **API de Microsoft**.

b. Elija **Microsoft Graph** → **Permisos de la aplicación** y, a continuación, elija el permiso que desea añadir.

c. Haga clic en el botón **Añadir permiso**.

Se añadirán los cuatro permisos, que aparecerán en la página **Permisos configurados**.

d. Haga clic en **Otorgar consentimiento de administrador para <tenant_name>** y, a continuación, en la ventana que se abre, haga clic en **Sí** a fin de brindar consentimiento para los permisos que añadió.

15. Vuelva a Kaspersky Security Center Cloud Console y, en la pestaña **General**, complete los siguientes campos obligatorios:
    - **Id. de inquilino**. El **ID del directorio (inquilino)** que copia en el paso 10.
    - **Id. del cliente**. El **ID de la aplicación (cliente)** que copia en el paso 10.
    - **Secreto del cliente**. El valor que copia en el paso 12.
16. Haga clic en el botón **Comprobar conexión** para comprobar si la configuración es correcta y, una vez que aparezca el estado **Conectado**, haga clic en el botón **Guardar**.

Se guarda la configuración de integración y se configura la integración con Microsoft Entra ID.

Después de configurar la integración con Microsoft Entra ID, debe hacer lo siguiente:

1. En el menú principal de Kaspersky Security Center Cloud Console, vaya a **Usuarios y funciones** → **Usuarios y grupos** para asegurarse de que los usuarios y grupos de Microsoft Entra ID se añadan a Kaspersky Security Center Cloud Console.

   Si los usuarios y los grupos en su inquilino de Microsoft Entra ID están sincronizados desde el Active Directory de la organización y el sondeo de Active Directory está configurado, los usuarios y los grupos ya se añadieron a Kaspersky Security Center Cloud Console como resultado del sondeo de Active Directory.

   De lo contrario, debe activar y ejecutar el sondeo de Microsoft Entra ID para añadir los usuarios y los grupos de su inquilino de Microsoft Entra ID a Kaspersky Security Center Cloud Console.

2. Asigne las funciones necesarios a los usuarios y los grupos.

   Para asignar funciones a un usuario en un Servidor de administración virtual, en el menú principal, vaya a **Usuarios y funciones** → **Usuarios y grupos**, y luego seleccione la pestaña **Usuarios**. Si selecciona la pestaña **Grupos** y, luego, asigna funciones al grupo en el que el usuario es miembro, el usuario no podrá iniciar sesión en Kaspersky Security Center Cloud Console.

3. Envíe la URL de inicio de sesión que copió en el paso 4 a los usuarios. Introducirán esta URL para **iniciar sesión en el espacio de trabajo de Kaspersky Security Center Cloud Console mediante sus credenciales de Microsoft**

Entra ID

Cuando un usuario cierra la sesión de la cuenta de Microsoft Entra ID que utilizó para la autenticación en Kaspersky Security Center Cloud Console, y Kaspersky Security Center Cloud Console está abierto en una pestaña o ventana diferente del mismo navegador, la sesión también finaliza para Kaspersky Security Center Cloud Console y el usuario sale automáticamente de la sesión de consola.

Si Kaspersky Security Center Cloud Console está abierto en otro navegador o en otros dispositivos, la sesión continúa cuando los usuarios cierran sesión en la cuenta de Microsoft Entra ID.

Para iniciar sesión en Kaspersky Security Center Cloud Console con las credenciales de la cuenta de Microsoft Entra ID, los usuarios deben ser capaces de iniciar sesión en su cuenta de Microsoft Entra ID.

Cómo activar el sondeo de Microsoft Entra ID

Debe activar el sondeo de Microsoft Entra ID para añadir a los usuarios de Microsoft Entra ID a Kaspersky Security Center Cloud Console.

Para activar el sondeo de Microsoft Entra ID, siga estos pasos:

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 **Microsoft Entra ID**.

3. En la sección **Detección de usuarios**, active el botón de **Sondeo de Microsoft Entra ID**.

4. Si desea cambiar la programación de sondeo predeterminada, haga clic en el botón **Configuración de programación**, especifique la frecuencia y la hora del sondeo en la ventana que se abre y, a continuación, haga clic en el botón **Guardar**.

   El sondeo de Microsoft Entra ID se ejecutará de acuerdo con la programación que configure.

5. Si desea ejecutar el sondeo de Microsoft Entra ID inmediatamente, haga clic en el botón **Ejecutar ahora**.

   Los usuarios se están cargando. Cuando se carguen los usuarios, finalizará el sondeo de Microsoft Entra ID.

6. Haga clic en el botón **Guardar**.

El sondeo de Microsoft Entra ID ha finalizado, y los usuarios de tu Microsoft Entra ID se añadieron a Kaspersky Security Center Cloud Console.

Añadir Kaspersky Security Center Cloud Console a la lista de aplicaciones

Para que los usuarios abran Kaspersky Security Center Cloud Console, permita que haga clic en el nombre de la aplicación en la lista sin introducir la URL de inicio de sesión. La lista de aplicaciones está disponible en Mis aplicaciones y el iniciador de Office 365.

Para añadir Kaspersky Security Center Cloud Console a la lista de aplicaciones:

1. En el menú principal del centro de administración de Microsoft Entra, vaya a **Identidad** → **Aplicaciones** → **Registros de apps** y, luego, en la pestaña **Todas las aplicaciones**, seleccione la aplicación Kaspersky Security Center Cloud Console que haya registrado previamente en Microsoft Entra ID.

2. En el menú de Kaspersky Security Center Cloud Console, seleccione la sección **Marca y propiedades** y, luego, siga estos pasos:

   a. En el campo **URL de la página de inicio**, introduzca la URL de inicio de sesión.

   b. Si es necesario, en el campo **Cargar nuevo logotipo**, añada una imagen que se utilizará como icono de la aplicación en la lista de aplicaciones.

   c. Haga clic en el botón **Guardar**.

3. En el menú principal del centro de administración de Microsoft Entra, vaya a **Identidad** → **Aplicaciones** → **Aplicaciones empresariales** y seleccione Kaspersky Security Center Cloud Console.

   Se abre la página de descripción general de la aplicación.

4. En el menú de Kaspersky Security Center Cloud Console, seleccione la sección **Propiedades** y, luego, siga estos pasos:

   a. Configure las siguientes opciones con la opción **Sí**:

   - **¿Activado para que los usuarios inicien sesión?**

     Esta acción solo es necesaria si la opción no está establecida en **Sí** de manera predeterminada.

   - **¿Visible para los usuarios?**

   b. Haga clic en el botón **Guardar**.

5. En el menú de Kaspersky Security Center Cloud Console, seleccione la sección **Usuarios y grupos** y, luego, siga estos pasos:

   a. Haga clic en el botón **Añadir usuario/grupo** y, luego, haga clic en el enlace debajo de **Usuarios y grupos**.

   b. En la ventana que se abre, seleccione usuarios y grupos y, luego, haga clic en el botón **Guardar**.

   Se cierra la ventana.

   c. Haga clic en el botón **Asignar**.

Kaspersky Security Center Cloud Console está disponible en Mis apps y el iniciador de Office 365 para los usuarios seleccionados. Para abrir Kaspersky Security Center Cloud Console, los usuarios pueden hacer clic en su nombre en la lista sin introducir la URL de inicio de sesión.

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.

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**.

Asignar a un usuario como propietario del dispositivo tras instalar el Agente de red

Para permitir que el usuario se registre como propietario de un dispositivo Linux:

1. En Kaspersky Security Center Web Console, vaya a **Detección y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**.

   Se abre la lista de paquetes de instalación.

2. Haga clic en el paquete de instalación del Agente de red.

   Se abrirá la ventana de propiedades del paquete de instalación elegido.

3. En la ventana de propiedades del paquete de instalación, haga clic en **Configuración** → **Avanzado**.

4. En la sección **Registro de usuario como propietario del dispositivo (solo Linux)**, active la opción **Permitir ejecutar la utilidad del registro de usuarios después de la instalación del Agente de red** y haga clic en **Guardar**.

La utilidad para registrar al usuario como propietario del dispositivo se puede ejecutar a través de la línea de comandos en el dispositivo cliente.

Para registrar un usuario como propietario de un dispositivo Linux en el dispositivo cliente:

1. Ejecute el siguiente comando en la línea de comandos en el dispositivo cliente:
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner`

2. Si se le solicita, introduzca el nombre de usuario y la contraseña.

   Si el inicio de sesión y la contraseña están incluidos en el archivo de respuesta o el paquete de instalación del Agente de red, ejecute el siguiente comando en la línea de comandos en el dispositivo cliente:
   `$ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended`

Si el usuario está incluido en un grupo de seguridad interno, el inicio de sesión debe contener el nombre de usuario.

Si el usuario está incluido en un grupo de seguridad de Active Directory, el inicio de sesión debe contener el nombre de usuario y el nombre de dominio.

El usuario quedará registrado como propietario del dispositivo.

Administración de revisiones de objetos

En esta sección encontrará información sobre la administración de revisiones de objetos. Kaspersky Security Center Cloud Console permite que usted siga la modificación de objeto. Cuando un objeto se modifica de algún modo, se crea una *revisión*. Cada revisión lleva un número que la identifica.

Los objetos que admiten administración de la revisión incluyen:

- Propiedades del Servidor de administración
- Directivas
- Tareas
- Grupos de administración
- Cuentas de usuario
- Paquetes de instalación

Puede realizar las siguientes acciones con las revisiones de los objetos:

- Ver una revisión seleccionada (disponible solo para directivas)
- Revertir los cambios realizados en un objeto a una revisión seleccionada
- Guardar revisiones como archivo JSON (disponible solo para directivas)

Todo objeto compatible con la administración de revisiones tiene una sección llamada **Historial de revisiones** en su ventana de propiedades. La sección contiene una lista de revisiones asociadas al objeto y los siguientes datos:

- **Revisión** número de revisión del objeto.
- **Hora** fecha y hora de modificación del objeto.
- **Usuario** nombre del usuario que modificó el objeto.
- **Dirección IP del dispositivo del usuario**: dirección IP del dispositivo desde el que se modificó el objeto.

- **Dirección IP de Web Console**: dirección IP de Kaspersky Security Center Web Console con la que se modificó el objeto.
- **Acción** acción realizada en el objeto.
- **Descripción** descripción de la revisión vinculada al cambio en la configuración del objeto.

  De forma predeterminada, la descripción de las revisiones está en blanco. Para agregar una descripción a una revisión, seleccione la revisión pertinente y haga clic en el botón **Editar descripción**. En la ventana abierta, ingrese el texto que describa la revisión.

Reversión de cambios

Los cambios realizados en un objeto pueden revertirse. Por ejemplo, puede volver a dejar la configuración de una directiva tal como estaba en una fecha puntual.

Para revertir los cambios realizados en un objeto:

1. En la ventana de propiedades del objeto, abra la pestaña **Historial de revisión**.
2. En la lista de revisiones del objeto, seleccione el número de revisión al que desee regresar.
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.

Agregar una descripción a una revisión

Para ayudarse a encontrar una revisión específica en la lista, puede agregarle una descripción.

Para agregar una descripción a una revisión:

1. En la ventana de propiedades del objeto, abra la pestaña **Historial de revisión**.
2. En la lista de revisiones del objeto, seleccione la revisión a la que desea agregar la descripción.
3. Haga clic en el botón **Editar descripción**.

   Se abre la ventana **Descripción**.
4. En la ventana **Descripción**, ingrese un texto que describa la revisión.

   De forma predeterminada, la descripción de las revisiones está en blanco.
5. Guarde la descripción de la revisión.

Se agrega la descripción a la revisión del objeto.

Ver y guardar una revisión de la directiva

Kaspersky Security Center Cloud Console le permite ver qué modificaciones se realizaron en una directiva durante un período determinado, así como guardar información sobre estas modificaciones en un archivo.

Ver y guardar una revisión de la directiva está disponible si el complemento web de administración correspondiente admite esta funcionalidad.

Para ver una revisión de la directiva:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en la directiva de la revisión que desea ver y vaya a la sección **Historial de revisión**.
3. En la lista de revisiones de la directiva, haga clic en el número de revisión que desea ver.

   Si el tamaño de la revisión es superior a 10 MB, no podrá verlo mediante Kaspersky Security Center Cloud Console. Se le pedirá que guarde la revisión seleccionada en un archivo JSON.

   Si el tamaño de la revisión no supera los 10 MB, se muestra un informe en formato HTML con la configuración de la revisión de la directiva seleccionada. Dado que el informe se muestra en una ventana emergente, asegúrese de que las ventanas emergentes estén permitidas en su navegador.

Para guardar una revisión de la directiva en un archivo JSON:

En la lista de revisiones de la directiva, seleccione la revisión que desea guardar y, luego, haga **Guardar en archivo**.

La revisión se guardará en un archivo JSON.

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.

Actualiza la funcionalidad (incluidas actualizaciones de firmas antivirus y actualizaciones de bases de código), además de la funcionalidad de KSN; puede no estar disponible en el software en los EE. UU.

Acerca de KSN

Kaspersky Security Network (KSN) es una infraestructura de servicios en línea que brinda acceso a la base de conocimientos en línea de Kaspersky, que contiene información sobre la reputación de los archivos, los recursos web y el software. El uso de los datos de Kaspersky Security Network garantiza una respuesta más rápida de las aplicaciones de Kaspersky ante las amenazas, mejora la eficacia de algunos componentes de protección y reduce el riesgo de falsos positivos. KSN permite utilizar las bases de datos de reputación de Kaspersky para obtener información sobre las aplicaciones instaladas en los dispositivos cliente.

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 Cloud Console. La información se transfiere de conformidad con la configuración de acceso a KSN. Los analistas de Kaspersky también analizan la información recibida y la incluyen en las bases de datos de reputación y de estadísticas de Kaspersky Security Network.

La aplicación le solicita que se una a KSN mientras se ejecuta el Asistente de inicio rápido. Puede iniciar o detener el uso de KSN en cualquier momento mientras usa 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 Cloud Console 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 habilitar el servidor proxy de KSN del lado del punto de distribución para hacer que el dispositivo actúe como proxy de KSN. En este caso, el servicio del proxy de KSN (ksnproxy) se ejecuta en el dispositivo.

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**, seleccione la sección **Configuración de KSN**.

3. Cambie el interruptor a la posición **Usar Kaspersky Security Network Activada**.

   KSN está activado.

   Si se habilita el botón de activación, los dispositivos cliente enviarán los resultados de instalación de parches a Kaspersky. Cuando active este botón de alternancia, deberá leer y aceptar los términos de la Declaración de KSN.

4. 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**, seleccione la sección **Configuración de KSN**.

3. Cambie el interruptor a la posición **Usar Kaspersky Security Network Desactivada**.

   KSN está desactivado.

   Si este botón de alternancia está desactivado, los dispositivos cliente no enviarán resultados de instalación de parches a Kaspersky.

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 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**, seleccione la sección **Configuración 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 muestra automáticamente cuando abre Kaspersky Security Center Cloud Console. 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. Puede ver y aceptar la Declaración de KSN actualizada 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 servidor proxy de KSN. Para funcionar como proxy de KSN, el dispositivo administrado debe tener activo el servicio ksnproxy. Puede verificar, activar o desactivar este servicio en el dispositivo localmente.

El dispositivo designado como punto de distribución puede utilizar Windows o Linux. El modo de llevar a cabo la verificación en el punto de distribución depende del sistema operativo instalado en el punto de distribución.

Para comprobar si el punto de distribución basado en Windows está operando como servidor proxy de KSN:

1. En el dispositivo de punto de distribución, en Windows, abra **Servicios** (**Todos los programas** → **Herramientas administrativas** → **Servicios**).

2. En la lista de servicios, verifique si el servicio ksnproxy se está ejecutando.

   Si el servicio ksnproxy se está ejecutando, entonces el Agente de red del dispositivo participa en Kaspersky Security Network y funciona como servidor proxy de KSN para los dispositivos administrados incluidos en el alcance del punto de distribución.

Si lo desea, puede desactivar el servicio ksnproxy. En este caso, el Agente de red del punto de distribución deja de participar en Kaspersky Security Network. Esto requiere derechos de administrador local.

Para verificar si un punto de distribución con Linux opera como servidor proxy de KSN:

1. En el dispositivo que actúe como punto de distribución, abra la lista de procesos en ejecución.

2. 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.

Eliminación de objetos

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 Cloud Console administra los dispositivos del grupo Dispositivos no asignados según las siguientes reglas:

- Si configuró reglas de movimiento de dispositivos y un dispositivo cumple con los criterios de una regla de movimiento, el dispositivo se mueve automáticamente a un grupo de administración de acuerdo con la regla.

- El dispositivo se almacena en el grupo de Dispositivos no asignados y se elimina automáticamente del grupo de acuerdo con las reglas de retención de dispositivos.

  Las reglas de retención de dispositivos no afectan a los dispositivos que tienen una o más unidades cifradas con cifrado de disco completo. Dichos dispositivos no se eliminan automáticamente, solo puede hacerlo de forma manual. Si necesita eliminar un dispositivo con una unidad cifrada, primero descifre la unidad y, luego, elimine el dispositivo.

  > Cuando elimina un dispositivo que tiene una unidad cifrada, también se eliminan los datos necesarios para descifrar la unidad. Si elige la casilla **Comprendo el riesgo y deseo eliminar el dispositivo** en la ventana de confirmación que se abre cuando elimina dichos dispositivos (del grupo **Dispositivos no asignados** o del grupo **Dispositivos administrados**), significa que es consciente de la subsiguiente eliminación de datos.

  En este caso, se deben cumplir las siguientes condiciones para descifrar la unidad:

  - 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.

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. Luego, si el dispositivo aún es visible para el Servidor de administración y ha configurado el sondeo de red regular, Kaspersky Security Center Cloud Console detecta el dispositivo durante el sondeo de red y lo añade de nuevo 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.

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 Cloud Console y las aplicaciones de seguridad

Actualiza la funcionalidad (incluidas actualizaciones de firmas antivirus y actualizaciones de bases de código), además de la funcionalidad de KSN; puede no estar disponible en el software en los EE. UU.

Escenario: actualización periódica de las 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. Después de completar el escenario de configuración de la protección de red, debe mantener la confiabilidad del sistema de protección. Este mantenimiento garantiza que la protección de los dispositivos administrados permanezca firme contra una variedad de amenazas, incluidos virus, ataques de red y ataques de phishing.

Hay varios esquemas que puede usar para instalar actualizaciones para los componentes de Kaspersky Security Center Cloud Console y las aplicaciones de seguridad. Elija uno o más esquemas que cumplan con los requisitos de su red.

El siguiente escenario describe el esquema de actualización que implica descargar actualizaciones a los repositorios de los puntos de distribución. Si los dispositivos administrados no tienen conexión a los puntos de distribución, considere la posibilidad de actualizar manualmente las bases de datos, los módulos de software y las aplicaciones de Kaspersky o realice la actualización directamente desde los servidores de actualización de Kaspersky.

Cuando completa este escenario, se producen los siguientes resultados:

- Los componentes de Kaspersky Security Center Cloud Console se actualizan automáticamente o solo cuando se designa el estado *Aprobado* para las actualizaciones.
- Las aplicaciones de seguridad de Kaspersky, las bases de datos de Kaspersky y los módulos de software se actualizan de acuerdo con la programación que especificó. De forma predeterminada, las aplicaciones de seguridad de Kaspersky instalan solo las actualizaciones que usted apruebe.

Puede configurar el proceso de actualización para descargar e instalar actualizaciones de dos maneras:

- Automáticamente

  En este caso, debe realizar este escenario solo una vez. Tendrá que programar la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* (si la hubiera) y las tareas de actualización de las aplicaciones de seguridad de Kaspersky, y mantener la configuración de actualización predeterminada que se encuentra en las propiedades del Agente de red.

- Manualmente

Puede configurar el proceso de actualización para ejecutar la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* (si la hay) y las tareas de actualización de las aplicaciones de seguridad de Kaspersky manualmente. También puede configurar el Agente de red para instalar las actualizaciones de los componentes de Kaspersky Security Center Cloud Console solo cuando designe el estado *Aprobado* para las actualizaciones.

Requisitos previos

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 Cloud Console. Al realizar este escenario, asignó una cantidad apropiada de puntos de distribución de acuerdo con la cantidad de dispositivos administrados y la topología de la red.

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.

Etapas

La configuración de la actualización con regularidad de las bases de datos y aplicaciones de Kaspersky se produce en etapas:

1. **Crear una tarea para descargar las actualizaciones en los repositorios de los puntos de distribución**

   Cree la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*. Cuando se ejecuta esta tarea, Kaspersky Security Center Cloud Console descarga las actualizaciones a los puntos de distribución directamente desde los servidores de actualización de Kaspersky.

   Instrucciones: Creación de la tarea para descargar actualizaciones en los repositorios de los puntos de distribución

2. **Configurar los puntos de distribución**

   Asegúrese de que la opción **Desplegar actualizaciones** esté activada en las propiedades de todos los puntos de distribución necesarios. Cuando esta opción está desactivada para un punto de distribución, los dispositivos incluidos en la cobertura del punto de distribución pueden descargar actualizaciones solo desde un recurso local o directamente desde los servidores de actualización de Kaspersky.

   Si desea que los dispositivos administrados reciban sus actualizaciones solamente de los puntos de distribución, habilite la opción **Distribuir archivos solo mediante puntos de distribución** en la directiva del Agente de red.

3. **Optimización del proceso de actualización mediante el uso de archivos diff (opcional)**

   Activar esta función reduce el tráfico entre 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 los repositorios de puntos de distribución*.

   Instrucciones: Uso de archivos diff para actualizar las bases de datos y módulos de software de Kaspersky

4. **Definir qué actualizaciones instalar**

   De forma predeterminada, las actualizaciones de software descargadas tienen el estado *Sin definir*. Cambie el estado a *Aprobado* o *Rechazado* para definir si esta actualización debe instalarse en los dispositivos en red. Las actualizaciones aprobadas siempre se instalan. Las actualizaciones no definidas solo se pueden instalar en el Agente de red y otros componentes de Kaspersky Security Center Cloud Console de acuerdo con la configuración de la directiva del Agente de red. Las actualizaciones a las que se les asigna el estado *Rechazada* no se instalan en los dispositivos.

   Instrucciones:

- Acerca de los estados de actualización
- Aprobar y rechazar actualizaciones de software

5. **Configuración de la instalación automática de actualizaciones y parches para componentes de Kaspersky Security Center Cloud Console**

   De manera predeterminada, las actualizaciones y los parches descargados para el Agente de red y otros componentes de Kaspersky Security Center Cloud Console se instalan automáticamente. Si deja habilitada la opción **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir** en las propiedades del Agente de red, se instalarán todas las actualizaciones que se descarguen en el repositorio (o en los repositorios). Si esta opción está desactivada, los parches de Kaspersky que se hayan descargado y etiquetado con el estado *Indeterminado* solo se instalarán después de que el administrador cambie su estado a *Aprobados*.

   Instrucciones: Habilitación y deshabilitación de actualizaciones automáticas y parches para componentes de Kaspersky Security Center Cloud Console

6. **Configurar la instalación automática de actualizaciones para las aplicaciones de seguridad**

   Cree tareas "Actualizar" para las aplicaciones administradas a fin de mantener al día las aplicaciones, los módulos de software y las bases de datos de Kaspersky (incluidas las bases de datos antivirus). Le recomendamos que seleccione la opción **Cuando se descarguen nuevas actualizaciones en el repositorio** al configurar el programa de tareas. Esto asegurará que se instalen nuevas actualizaciones lo antes posible.

   De manera predeterminada, las actualizaciones para las aplicaciones administradas se instalan solo después de que cambia el estado de actualización a *Aprobado*. Para Kaspersky Endpoint Security para Windows, puede cambiar la configuración de actualización en la tarea Actualizar.

   Si una actualización exige revisar y aceptar los términos del Contrato de licencia de usuario final, es necesario aceptar esos términos para proceder con la instalación. Una vez que se aceptan los términos, la actualización se puede propagar a los dispositivos administrados.

   Instrucciones: Instalación automática de actualizaciones de Kaspersky Endpoint Security en dispositivos

7. **Aprobar y rechazar actualizaciones de aplicaciones de Kaspersky administradas**

   De forma predeterminada, las actualizaciones de software descargadas tienen el estado *Sin definir*. Puede cambiar este estado a *Aprobada* o *Rechazada*. Las actualizaciones aprobadas siempre se instalan. Si una actualización de una aplicación Kaspersky gestionada exige revisar y aceptar los términos del Contrato de licencia de usuario final, es necesario aceptar esos términos para proceder con la instalación. Una vez que se aceptan los términos, la actualización se puede propagar a los dispositivos administrados. Las actualizaciones a las que se les asigna el estado *Rechazada* no se instalan en los dispositivos. Si previamente ha instalado una actualización rechazada para una aplicación administrada, Kaspersky Security Center Cloud Console intentará desinstalar la actualización de todos los dispositivos.

   Aprobar y rechazar actualizaciones solo está disponible para el Agente de red y las aplicaciones Kaspersky administradas instaladas en dispositivos cliente basados en Windows y en Linux. No se admite la actualización sin interrupciones del Servidor de administración, Kaspersky Security Center Cloud Console y los complementos web de administración.

   Instrucciones: aprobar y rechazar actualizaciones de software

Al finalizar el escenario, puede proceder a 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 dispositivos administrados está actualizada, debe tener siempre actualizado lo siguiente:

- 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 Cloud Console 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 Cloud Console y las aplicaciones de seguridad

  Kaspersky Security Center Cloud Console le permite actualizar el Agente de red y las aplicaciones de Kaspersky instaladas en dispositivos cliente basados en Windows y en Linux automáticamente. No se admite la actualización sin interrupciones del Servidor de administración, Kaspersky Security Center Cloud Console y los complementos web de administración. Para actualizar estos componentes, debe descargar las últimas versiones desde el sitio web de Kaspersky e instalarlas manualmente.

Existen distintos esquemas para descargar las actualizaciones necesarias y distribuirlas a los dispositivos administrados. La elección de una u otra opción depende de la configuración de la red. Estas son las posibilidades:

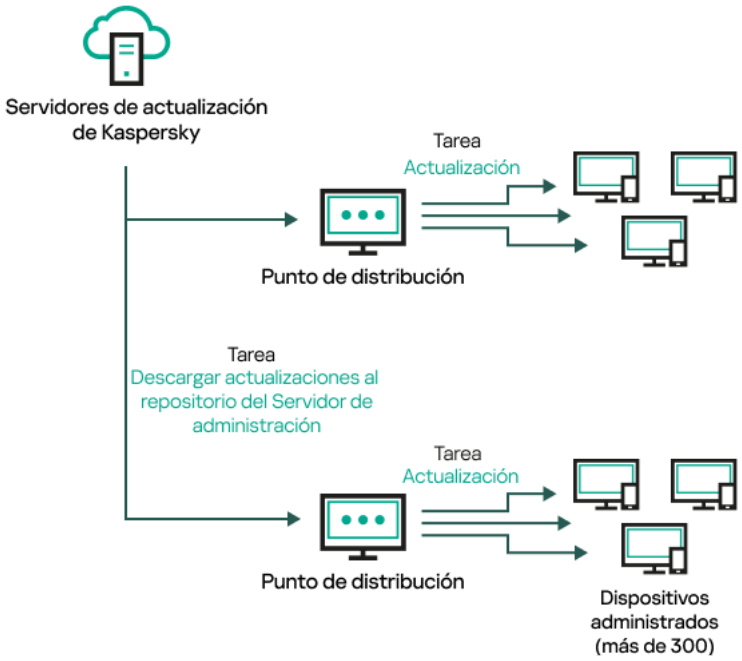
- Uso de la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*
- Utilizar una carpeta local, una carpeta compartida o un servidor FTP (método manual)
- Directamente desde los servidores de actualización de Kaspersky a las aplicaciones de seguridad en los dispositivos administrados

Utilizar la tarea Descargar actualizaciones en los repositorios de puntos de distribución

En este esquema, Kaspersky Security Center Cloud Console descarga actualizaciones a través de la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*. Los dispositivos administrados incluidos en la cobertura de un punto de distribución descargan las actualizaciones desde el repositorio de puntos de distribución (consulte la figura a continuación).

Los puntos de distribución con macOS no pueden descargar actualizaciones de los servidores de actualizaciones de Kaspersky.

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



Actualización mediante el uso de la tarea Descargar actualizaciones en los repositorios de puntos de distribución

Una vez que se completa la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*, las siguientes actualizaciones se descargan en el repositorio de los puntos de distribución:

- Bases de datos y módulos de software de Kaspersky para las aplicaciones de seguridad instaladas en los dispositivos administrados

  Estas actualizaciones se instalan a través de la tarea "Actualizar" de Kaspersky Endpoint Security para Windows.

- Actualizaciones para los componentes de Kaspersky Security Center Cloud Console

  Por defecto, estas actualizaciones se instalan automáticamente. Puede cambiar este comportamiento en la directiva del Agente de red.

- Actualizaciones para las aplicaciones de seguridad

  De forma predeterminada, Kaspersky Endpoint Security para Windows instala solo las actualizaciones que usted apruebe. Las actualizaciones se instalan a través de la tarea "Actualizar" y se pueden configurar en las propiedades de dicha tarea.

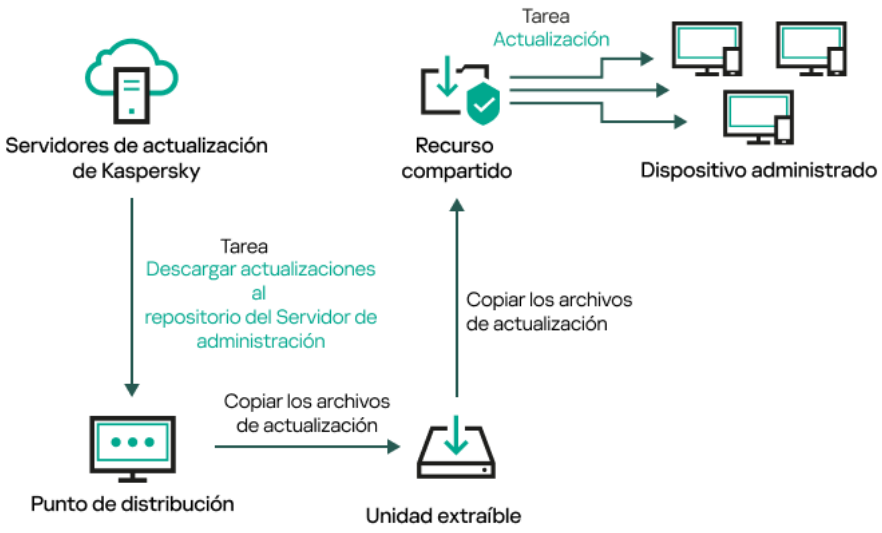
Cada aplicación de Kaspersky le solicita al Servidor de administración las actualizaciones que requiere. El Servidor de administración combina estas solicitudes y descarga a los repositorios de puntos de distribución solo aquellas actualizaciones solicitadas por los programas. De este modo, se evita 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 los repositorios de puntos de distribución*, el Servidor de administración envía la siguiente información a los servidores de actualizaciones de Kaspersky automáticamente:

- Id. y versión de la aplicación
- Id. de instalación de la aplicación
- Id. de la clave activa
- Tarea de descarga e id. de ejecución

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 una carpeta local, una carpeta compartida o un servidor FTP (método manual)

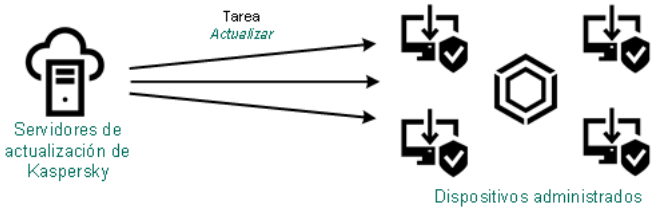
Si los dispositivos cliente no tienen una conexión con un punto de distribución, puede usar una carpeta local o un recurso compartido como fuente para actualizar bases de datos, módulos de software y aplicaciones de Kaspersky. En este esquema, tiene que copiar las actualizaciones requeridas (desde un repositorio de puntos de distribución a una unidad extraíble) y después copiar las actualizaciones a la carpeta local o al recurso compartido especificado como origen de actualizaciones en la configuración de Kaspersky Endpoint Security para Windows (consulte la siguiente figura).



Actualización con una carpeta local, una carpeta compartida o un servidor FTP

Directamente desde los servidores de actualización de Kaspersky a Kaspersky Endpoint Security para Windows en los dispositivos administrados

En los dispositivos administrados, puede configurar Kaspersky Endpoint Security para Windows para recibir actualizaciones directamente desde los servidores de actualización de Kaspersky (ver la siguiente figura).



Actualización directa de las aplicaciones de seguridad utilizando los servidores de actualizaciones de Kaspersky

En este esquema, la aplicación de seguridad no utiliza los repositorios proporcionados por Kaspersky Security Center Cloud Console. Para que las actualizaciones se descarguen directamente de los servidores de actualizaciones de Kaspersky, deberá definir esos servidores como origen de actualizaciones en la interfaz de la aplicación de seguridad. Para obtener una descripción completa de estos ajustes, consulte la documentación de Kaspersky Endpoint Security para Windows.

Crear una tarea para descargar las actualizaciones en los repositorios de los puntos de distribución

Los puntos de distribución con macOS no pueden descargar actualizaciones de los servidores de actualizaciones de Kaspersky.

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

Puede crear la tarea *Descargar actualizaciones en los repositorios de 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.

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 de los componentes de Kaspersky Security Center Cloud Console.
- 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, haga lo siguiente:

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 Cloud Console, 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 activa la opción **Abrir los detalles de la tarea cuando se complete la creación**, puede modificar la configuración de tareas predeterminada. 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. La carpeta de red puede ser un servidor FTP o HTTP, o un recurso compartido SMB. Si el acceso a la carpeta requiere autenticación, solo puede usarse el protocolo SMB. La carpeta local debe ser una carpeta del dispositivo en el que se encuentra instalado el Servidor de administración.

  El servidor FTP/HTTP o la carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura que se crea al usar los servidores de actualizaciones de Kaspersky.

- **Carpeta para almacenar actualizaciones**

  La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta especificada en el portapapeles. No puede cambiar la ruta a una carpeta específica para una tarea de grupo.

- **Descargar archivos 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**

Kaspersky Security Center Cloud Console descarga actualizaciones de bases de datos y 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 13.2 o una versión anterior

Suponga, por ejemplo, que un punto de distribución está configurado para tomar las actualizaciones de una carpeta local o de red. En ese caso, puede utilizar un Servidor de administración que tenga conexión a Internet para descargar las actualizaciones y colocar los archivos descargados en la carpeta local del punto de distribución. Si el Servidor de administración es de versión 13.2 o anterior, habilite la opción **Descargar actualizaciones utilizando el esquema anterior** en la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*.

Esta opción está deshabilitada de manera predeterminada.

10. Programe la ejecución de la tarea. De ser necesario, configure los siguientes ajustes:

- **Iniciar tarea**

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - **Manualmente** (seleccionado de manera predeterminada)

    La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

    Esta opción está seleccionada 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 manera 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 Cloud Console.

  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.

  De manera predeterminada, no se selecciona ningún día del mes. La hora de inicio predeterminada es a las 18:00.

- **Al detectar un brote de virus**

La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

- Antivirus para estaciones de trabajo y servidores de archivos
- Antivirus para defensa del perímetro
- Antivirus para sistemas de correo

Por defecto, están seleccionados todos los tipos de aplicaciones.

En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completar otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. Este parámetro solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Se completó correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Introduzca el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el icono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el icono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **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 las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manualmente**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de manera predeterminada.

- **Usar el retraso aleatorio automáticamente para el inicio de la tarea**

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- Usar el retraso aleatorio automáticamente para el inicio de la tarea con un intervalo de

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está deshabilitada de 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.

Configuración de los dispositivos administrados para recibir actualizaciones solo desde los puntos de distribución

Los dispositivos administrados pueden recuperar las actualizaciones de las bases de datos de Kaspersky, los módulos de software y las aplicaciones de Kaspersky de varias fuentes: directamente desde los servidores de actualización, los puntos de distribución o una carpeta local o de red. Puede especificar puntos de distribución como la única fuente posible de actualizaciones.

Para configurar los dispositivos administrados a fin de recibir actualizaciones solo desde los puntos de distribución:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en la directiva del Agente de red.

3. En la ventana de propiedades de la directiva, vaya a la pestaña **Configuración de la aplicación**.

4. En la sección **Configuración**, active el botón de activación **Distribuir archivos solo mediante puntos de distribución**.

5. Bloquee (🔒) el interruptor.

6. Haga clic en el botón **Guardar**.

La directiva se aplicará a los dispositivos seleccionados, y los dispositivos recibirán actualizaciones solo desde los puntos de distribución.

Habilitación y deshabilitación de actualizaciones automáticas y parches para componentes de Kaspersky Security Center Cloud Console

La instalación automática de actualizaciones y parches para componentes de Kaspersky Security Center Cloud Console está habilitada de forma predeterminada durante la instalación del Agente de red en el dispositivo. Puede deshabilitarla durante la instalación del Agente de red o puede hacerlo más adelante usando una directiva.

Para deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center Cloud Console durante instalación local del Agente de red en un dispositivo, realice lo siguiente:

1. Inicie la instalación local del Agente de red en el dispositivo.

2. En el paso **Configuración avanzada**, desactive la casilla **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes**.

3. Siga las instrucciones del asistente.

Se instalará el Agente de red con la actualización automática y los parches para componentes de Kaspersky Security Center Cloud Console deshabilitados en el dispositivo. Si desea habilitar la autoinstalación de actualizaciones y parches más adelante, podrá hacerlo a través de una directiva.

Para deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center Cloud Console durante la instalación del Agente de red en el dispositivo mediante un paquete de instalación, realice lo siguiente:

1. En el menú principal, vaya a **Operaciones → Repositorios → Paquetes de instalación**.

2. Haga clic en el paquete **Agente de red de Kaspersky Security Center <número de versión>**.

3. En la ventana propiedades, seleccione la pestaña **Configuración**.

4. Desactive el interruptor **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir**.

Se instalará el Agente de red con la actualización automática y los parches para componentes de Kaspersky Security Center Cloud Console deshabilitados de este paquete. Si desea habilitar la autoinstalación de actualizaciones y parches más adelante, podrá hacerlo a través de una directiva.

Si se seleccionó (o se desactivó) la casilla en el paso 4 durante la instalación del Agente de red en el dispositivo, puede habilitar (o deshabilitar) posteriormente la actualización automática usando la directiva del Agente de red.

Para habilitar o deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center Cloud Console usando la directiva del Agente de red, realice lo siguiente:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en la directiva del Agente de red.
3. En la ventana de propiedades de la directiva, seleccione la pestaña **Configuración de la aplicación**.
4. En la sección **Administrar parches y actualizaciones**, active o desactive el interruptor **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir** para habilitar o deshabilitar, respectivamente, la instalación automática de actualizaciones y parches.
5. Asegúrese de establecer (**Aplicar**) el bloqueo (🔒) con este botón de activación.

La directiva se aplicará a los dispositivos seleccionados y la actualización automática y los parches para los componentes de Kaspersky Security Center Cloud Console se habilitarán (o se deshabilitarán) en estos dispositivos.

Instalación automática de actualizaciones para Kaspersky Endpoint Security para Windows

Puede hacer que las bases de datos y los módulos de software de Kaspersky Endpoint Security para Windows se actualicen automáticamente en los dispositivos cliente.

Para que las actualizaciones de Kaspersky Endpoint Security para Windows se descarguen y se instalen automáticamente en los dispositivos cliente, haga lo siguiente:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en el botón **Añadir**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. Busque la aplicación Kaspersky Endpoint Security para Windows y seleccione **Actualizar** como subtipo de tarea.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Elija el alcance de la tarea.
6. Elija el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplicará la tarea.
7. En el paso **Finalizar la creación de tareas**, si activa la opción **Abrir los detalles de la tarea cuando se complete la creación**, puede modificar la configuración de tareas predeterminada. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.
8. Haga clic en el botón **Crear**.

   Se crea la tarea y se la agrega a la lista de tareas.
9. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

10. En la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea, defina la configuración de la tarea de actualización en modo local o modo móvil:

    - **Modo local**: las opciones de esta pestaña definen de qué modo el dispositivo recibe actualizaciones cuando se establece la conexión entre el dispositivo y el Servidor de administración.

    - **Modo móvil**: las opciones de esta pestaña definen de qué modo el dispositivo recibe actualizaciones cuando no se establece una conexión entre Kaspersky Security Center Cloud Console y el dispositivo (por ejemplo, cuando el dispositivo no está conectado a Internet).

11. Habilite los orígenes de actualizaciones que desee usar para actualizar las bases de datos y los módulos de Kaspersky Endpoint Security para Windows. Si es necesario, cambie las posiciones de las fuentes en la lista usando los botones **Subir** y **Bajar**. Si habilita más de un origen de actualizaciones, Kaspersky Endpoint Security para Windows intentará conectarse a ellos en orden, uno tras otro, comenzando por el primero de la lista. La tarea de actualización descargará el paquete de actualización del primer origen disponible.

    Cuando Kaspersky Security Center Cloud Console se configura como un origen de actualizaciones, las actualizaciones se descargan desde el repositorio de un punto de distribución, no desde el repositorio del Servidor de administración. Asegúrese de asignar puntos de distribución y crear la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*.

12. Habilite la opción **Instalar actualizaciones aprobadas para los módulos de la aplicación** para que, junto con las bases de datos de la aplicación, se descarguen también las actualizaciones para los módulos de software.

    Si habilita esta opción, Kaspersky Endpoint Security para Windows le informará al usuario sobre la disponibilidad de actualizaciones para los módulos de software. Cuando se ejecute la tarea de actualización, estas actualizaciones se incluirán en el paquete de actualización. Kaspersky Endpoint Security para Windows instala solo aquellas actualizaciones para las cuales ha establecido el estado *Aprobado*; se instalarán localmente a través de la interfaz de la aplicación o de Kaspersky Security Center Cloud Console.

    También puede habilitar la opción **Instalar automáticamente actualizaciones de módulos críticas**. Cuando haya actualizaciones disponibles para los módulos de software, Kaspersky Endpoint Security para Windows instalará automáticamente las que tengan estado *Crítico*; las demás actualizaciones se instalarán cuando usted las apruebe.

    Para actualizar los módulos de software, podría resultar necesario leer y aceptar los términos del contrato de licencia y de la política de privacidad. Cuando este sea el caso, la aplicación esperará a que el usuario acepte los términos de estos documentos y luego instalará las actualizaciones.

13. Active la casilla de verificación **Copiar actualizaciones a la siguiente carpeta** para que la aplicación guarde las actualizaciones descargadas en una carpeta. A continuación, elija la carpeta de destino.

14. Defina una programación para la tarea. Recomendamos seleccionar la opción **Al descargar nuevas actualizaciones al repositorio** de manera que las actualizaciones se instalen sin demora.

15. Haga clic en **Guardar**.

Cuando la tarea **Actualizar** está en ejecución, la aplicación envía solicitudes a los servidores de actualizaciones de Kaspersky.

Algunas actualizaciones requieren que estén instaladas las últimas versiones de los complementos de administración.

Acerca de los estados de actualización

El *estado* es un atributo de las actualizaciones de software que define si una actualización de software en particular debe instalarse en un dispositivo en red.

Una actualización puede tener los siguientes estados:

- *Sin definir*

  De forma predeterminada, las actualizaciones de software descargadas tienen el estado *Sin definir*. Las actualizaciones no definidas solo se pueden instalar en el Agente de red y otros componentes de Kaspersky Security Center Cloud Console de acuerdo con la configuración de la directiva del Agente de red.

- *Aprobada*

  Las actualizaciones aprobadas siempre se instalan. Si una actualización exige revisar y aceptar los términos del Contrato de licencia de usuario final, es necesario aceptar esos términos para proceder con la instalación.

- *Rechazada*

  Las actualizaciones a las que se les asigna el estado *Rechazada* no se instalan en los dispositivos.

Puede cambiar los estados de las actualizaciones para los siguientes softwares:

- El Agente de red y otros componentes de Kaspersky Security Center Cloud Console

  De manera predeterminada, las actualizaciones y los parches descargados para los componentes de Kaspersky Security Center Cloud Console se instalan automáticamente. Si deja habilitada la opción **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir** en las propiedades del Agente de red, se instalarán todas las actualizaciones que se descarguen en el repositorio (o en los repositorios). Si esta opción está desactivada, los parches de Kaspersky que se hayan descargado y etiquetado con el estado *Indeterminado* solo se instalarán después de que el administrador cambie su estado a *Aprobados*.

  Las actualizaciones para los componentes de Kaspersky Security Center Cloud Console no se pueden desinstalar, incluso si establece el estado *Rechazada* para una actualización.

- Aplicaciones de seguridad de Kaspersky

  De manera predeterminada, las actualizaciones para las aplicaciones administradas se instalan solo después de que cambia el estado de actualización a *Aprobado*. Si previamente se instaló una actualización rechazada para una aplicación de seguridad, Kaspersky Security Center Cloud Console intentará desinstalar la actualización de todos los dispositivos.

Aprobar y rechazar actualizaciones de software

Una tarea de instalación de actualizaciones puede estar configurada para requerir la aprobación de las actualizaciones que se deban instalar. Puede aprobar las actualizaciones que deban instalarse y rechazar las que no deban instalarse.

Podría suceder, por ejemplo, que quiera instalar las actualizaciones en un entorno de prueba para verificar primero que no interfieran con el funcionamiento de los dispositivos, y solo entonces, en caso de no haber problemas, permitir que se instalen en los dispositivos cliente.

Aprobar y rechazar actualizaciones solo está disponible para el Agente de red y las aplicaciones administradas instaladas en dispositivos cliente basados en Windows y en Linux. No se admite la actualización sin interrupciones del Servidor de administración, Kaspersky Security Center Cloud Console y los complementos web de administración. Para actualizar estos componentes, debe descargar las últimas versiones desde el sitio web de Kaspersky e instalarlas manualmente.

Para aprobar o rechazar una o más actualizaciones:

1. En el menú principal, vaya a **Operaciones → Aplicaciones de Kaspersky → Actualizaciones sin interrupciones**.

   Aparece una lista con las actualizaciones disponibles.

   Las actualizaciones para las aplicaciones administradas pueden requerir que la versión de Kaspersky Security Center instalada no sea anterior a una versión en particular. Si está utilizando una versión anterior a la necesaria, podrá ver tales actualizaciones, pero no las podrá aprobar. Tampoco podrá crear paquetes de instalación a partir de esas actualizaciones hasta que actualice Kaspersky Security Center. De intentarlo, se le pedirá que actualice su copia de Kaspersky Security Center a la versión mínima requerida.

2. Si es necesario, acepte el EULA haciendo clic en el botón **Ver y aceptar contratos de licencia**.

3. Seleccione las actualizaciones que desee aprobar o rechazar.

4. Haga clic en **Aprobar** para aprobar las actualizaciones seleccionadas o en **Rechazar** para rechazarlas.

   El valor predeterminado es *Sin definir*.

Las actualizaciones a las que les haya asignado el estado *Aprobada* se pondrán en una cola para ser instaladas.

Las actualizaciones a las que les haya asignado el estado *Rechazada* se desinstalarán (si tal acción es posible) de todos los dispositivos en los que estén instaladas. Estas actualizaciones no se instalarán en otros dispositivos en el futuro.

Existen actualizaciones para las aplicaciones de Kaspersky que no se pueden desinstalar. Si configura el estado *Rechazada* para ellas, Kaspersky Security Center Cloud Console no desinstalará estas actualizaciones de los dispositivos en los cuales se hayan instalado anteriormente. Sin embargo, se abstendrá de instalarlas en otros dispositivos en el futuro.

Si asigna el estado *Rechazada* a las actualizaciones de software de un tercero, estas no se instalarán en los dispositivos a los que estén asignadas, pero que aún no las hayan recibido. Las actualizaciones no se borrarán de los dispositivos en los que ya se encuentren instaladas. Si necesita eliminarlas, deberá hacerlo manualmente, en forma local.

Usar archivos diff para actualizar las bases de datos y los 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. El uso de archivos diff limita el 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 activada en un punto de distribución, los archivos diff se guardan en este punto de distribución. Como resultado, los dispositivos que toman actualizaciones de este 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 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 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.

Para activar la función de descarga de archivos diff:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* para abrir las propiedades de la tarea.
3. En la pestaña **Configuración de la aplicación**, habilite la opción **Descargar archivos de comparación**.
4. Haga clic en el botón **Guardar**.

   La función Descargar archivos diff se activa. Se descargarán archivos diff de actualizaciones además de los archivos de actualización cada vez que se ejecuta la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*.

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.

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 repositorios de puntos de distribución.

Cuando necesite actualizar las bases de datos y los módulos de software en un dispositivo (o un grupo de dispositivos) que no esté conectado 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 las siguientes fuentes:

- Punto de distribución.

Para asegurarse de que el repositorio del punto de distribución contenga las actualizaciones necesarias para la aplicación de seguridad instalada en un dispositivo desconectado, al menos uno de los dispositivos en línea administrados en la cobertura del punto de distribución debe tener la misma aplicación de seguridad instalada. Esta aplicación debe estar configurada para recibir las actualizaciones desde el repositorio del punto de distribución mediante la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*.

- Cualquier dispositivo que tenga la misma aplicación de seguridad instalada y configurada para recibir las actualizaciones desde 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 de punto de distribución.

Para actualizar las bases de datos y los módulos de software de Kaspersky en dispositivos sin conexión:

1. Conecte la unidad extraíble al dispositivo de punto de distribución.
2. Copie los archivos de las actualizaciones a la unidad extraíble.

   De manera predeterminada, las actualizaciones se encuentran en: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\Updates.
3. En los dispositivos sin conexión, configure la aplicación de seguridad (por ejemplo, Kaspersky Endpoint Security para Windows) para que obtenga sus actualizaciones de una carpeta local o de un recurso compartido (por ejemplo, una carpeta compartida o un servidor FTP).
4. Copie los archivos de las actualizaciones de la unidad extraíble a la carpeta local o al recurso compartido que quiera usar como origen de actualizaciones.
5. En el dispositivo sin conexión en el que se deban instalar las actualizaciones, inicie la tarea de actualización de Kaspersky Endpoint Security para Windows.

Cuando se complete la tarea de actualización, el dispositivo tendrá las bases de datos y los módulos de software de Kaspersky más recientes.

Actualización de las bases de datos de Kaspersky Security for Windows Server

Puede instalar Kaspersky Security for Windows Server en dispositivos administrados y es posible que desee iniciar la tarea Protección de archivos en tiempo real de esta aplicación. Sin embargo, la aplicación viene sin las bases de datos necesarias para su correcto funcionamiento. Las bases de datos se descargan en el dispositivo administrado solo después de completarse la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*.

Si desea iniciar la tarea Protección de archivos en tiempo real en un dispositivo administrado inmediatamente después de instalar Kaspersky Security for Windows Server en él, debe asegurarse de que las bases de datos para esa aplicación estén descargadas y actualizadas. De lo contrario, la tarea podría funcionar incorrectamente.

Para asegurarse de que las bases de datos de Kaspersky Security for Windows Server estén actualizadas:

1. Asegúrese de que la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* se haya completado en el Servidor de administración.
2. Realice una de las siguientes acciones:

- En la configuración de la tarea Protección de archivos en tiempo real, seleccione la opción de inicio **Al iniciar la aplicación** y, luego, reinicie el dispositivo administrado.

- En la configuración de la tarea Protección de archivos en tiempo real, defina manualmente la hora de inicio a la hora que desee.

La tarea Protección de archivos en tiempo real en Kaspersky Security for Windows Server está lista para funcionar correctamente.

Administración de aplicaciones de terceros en dispositivos cliente

Esta sección describe las funciones de Kaspersky Security Center Cloud Console relacionadas con la administración de aplicaciones de terceros instaladas en dispositivos cliente.

Limitaciones de Administración de vulnerabilidades y parches

La función Administración de vulnerabilidades y parches tiene una serie de limitaciones, según la licencia que utilice y el modo en el que Kaspersky Security Center Cloud Console esté funcionando.

Las siguientes licencias no son compatibles con la Administración de vulnerabilidades y parches:

- Kaspersky Endpoint Security for Business Select
- Kaspersky Hybrid Cloud Security

Las siguientes licencias admiten Administración de vulnerabilidades y parches:

- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Total Security for Business
- Kaspersky Hybrid Cloud Security Enterprise

La siguiente tabla compara las limitaciones de Kaspersky Security Center Cloud Console en el modo de prueba, bajo licencias que no admiten Administración de vulnerabilidades y parches, y bajo licencias que la admiten.

Limitaciones de Administración de vulnerabilidades y parches

Limitación	Modo de prueba	Modo comercial: licencias que no admiten Administración de vulnerabilidades y parches	Modo comercial: licencias que admiten Administración de vulnerabilidades y parches
Número máximo de tareas *Instalar actualizaciones de Windows Update* o tareas *Reparar vulnerabilidades*	4	4	0 (no se pueden crear nuevas tareas de estos tipos)
Número máximo de tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades*	2	No admitido	4
Número máximo de reglas en todos las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades*	10	No admitido	50
Número máximo de actualizaciones de software que pueden tener el estado *Aprobada* al mismo tiempo en todos los servidores, incluidos los virtuales	100	No admitido	1000
Cantidad máxima de actualizaciones de software que se pueden añadir manualmente a una tarea, en todos los servidores, incluidos los virtuales	500	1000	1000
Cantidad máxima de vulnerabilidades de software que se pueden añadir manualmente a una tarea, en todos los servidores, incluidos los virtuales	500	1000	1000

Disponibilidad de funciones Administración de vulnerabilidades y parches en modo comercial y de prueba y bajo varias opciones de licencia

La disponibilidad de las funciones de Administración de vulnerabilidades y parches en Kaspersky Security Center Cloud Console depende de si la usa en modo de prueba o comercial, así como de la opción de licencia que ha seleccionado. Utilice la tabla para verificar qué funciones de Administración de vulnerabilidades y parches están disponibles.

Disponibilidad de funciones Administración de vulnerabilidades y parches

Función Administración de vulnerabilidades y parches	Modo de prueba	Modo comercial: Kaspersky Endpoint Security for Business Select	Modo comercial: Kaspersky Endpoint Security for Business Advanced, Kaspersky Endpoint Detection and Response Optimum, Kaspersky Total Security for Business
Corrección manual de vulnerabilidades en el software de Microsoft en dispositivos administrados que ejecutan Windows Creación de la tarea *Reparar vulnerabilidades*	✓	✓	—
Instalación manual de actualizaciones en el software de Microsoft en dispositivos administrados que ejecutan Windows Instalación de actualizaciones de software de terceros a través de la tarea *Instalar actualizaciones de Windows Update*	—	✓	✓
Instalación automática basada en reglas de actualizaciones de software de terceros y reparación de vulnerabilidades de software de terceros Crear la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* e instalar las actualizaciones Agregar reglas de instalación de actualizaciones	✓	—	✓

Acerca de las aplicaciones de terceros

Kaspersky Security Center Cloud Console puede ayudarlo a actualizar el software de terceros instalado en los dispositivos de los clientes y a corregir las vulnerabilidades del software de terceros. Kaspersky Security Center Cloud Console solo puede actualizar el software de terceros de la versión actual a la versión más reciente.

La lista de software de terceros está sujeta a cambios. Podrían agregarse nuevas aplicaciones en el futuro. Puede comprobar si puede actualizar el software de terceros (instalado en los dispositivos de los usuarios) con Kaspersky Security Center Cloud Console consultando la lista de actualizaciones disponibles en Kaspersky Security Center Cloud Console.

El procedimiento que se describe a continuación está destinado únicamente a ver la lista de software de terceros que se puede actualizar con Kaspersky Security Center Cloud Console. Se siguen los pasos para acceder a la información relevante sin iniciar ninguna tarea.

Para ver la lista de software de terceros que puede actualizar con Kaspersky Security Center Cloud Console, haga lo siguiente:

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 el paso **Configuración de tarea nueva** del asistente, especifique estos ajustes:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Security Center Cloud Console**.

   b. En el campo **Tipo de tarea**, elija **Instalar actualizaciones requeridas y reparar vulnerabilidades**.

4. En el paso **Cobertura de la tarea** del asistente, seleccione la opción **Dispositivos administrados**.

5. En el paso del asistente **Especificar reglas para instalar actualizaciones**, haga clic en el botón **Añadir**.

   Se inicia el Asistente de creación de reglas. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

6. En el paso del asistente **Seleccionar tipo de regla**, elija **Regla para actualizaciones de terceros**.

7. En el paso del asistente **Criterios generales**, elija la opción **Instalar todas las actualizaciones (excepto las rechazadas)** y, luego, haga clic en **Siguiente**.

Se muestra la lista de software de terceros.

Actualizaciones para el software de terceros

Kaspersky Security Center Cloud Console le permite administrar las actualizaciones de software de terceros instaladas en los dispositivos administrados y reparar vulnerabilidades en las aplicaciones de Microsoft y los productos de otros desarrolladores de software mediante la instalación de las actualizaciones requeridas.

Kaspersky Security Center Cloud Console busca actualizaciones a través de la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, el Servidor de administración recibe listas en las que se detallan las vulnerabilidades detectadas y las actualizaciones requeridas para el software de terceros con el que cuentan los dispositivos indicados en las propiedades de la tarea. Tras ver la información de las actualizaciones disponibles, puede instalarlas en los dispositivos.

Kaspersky Security Center Cloud Console actualiza algunas aplicaciones quitando la versión anterior de la aplicación e instalando la nueva.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedírsele al usuario que la cierre.

Por razones de seguridad, las tecnologías de Kaspersky analizan automáticamente en busca de malware cualquier actualización de software de terceros que instale mediante la función Administración de vulnerabilidades y parches. Estas tecnologías se utilizan para la verificación automática de archivos e incluyen análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno de pruebas y aprendizaje automático.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. Además, los expertos de Kaspersky no buscan vulnerabilidades (conocidas o desconocidas) ni funciones no documentadas en dichas actualizaciones, ni realizan otros tipos de análisis de las actualizaciones distintos a los especificados en el párrafo anterior.

Tareas para la instalación de actualizaciones de software de terceros

Una vez que los metadatos de las actualizaciones de software de terceros se descargan al repositorio, puede usar las siguientes tareas para instalar las actualizaciones en los dispositivos cliente:

- La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*

  Esta tarea se utiliza para instalar actualizaciones para aplicaciones de Microsoft, incluidas las actualizaciones suministradas por el servicio de Windows Update, y actualizaciones de productos de otros proveedores.

  Cuando se completa esta tarea, las actualizaciones se instalan en los dispositivos administrados automáticamente. Cuando se descargan metadatos de nuevas actualizaciones en el repositorio del Servidor de administración, Kaspersky Security Center Cloud Console verifica si estas actualizaciones cumplen con los criterios especificados en las reglas de actualización. Las actualizaciones nuevas que cumplen con los criterios se descargan e instalan en forma automática cuando la tarea se ejecuta nuevamente.

- La tarea *Instalar actualizaciones de Windows Update*

  Esta tarea solo puede usarse para instalar actualizaciones de Windows Update.

  Cuando se completa esta tarea, se instalan únicamente las actualizaciones especificadas en sus propiedades. En el futuro, si desea instalar nuevas actualizaciones, debe añadir las actualizaciones necesarias a la lista de actualizaciones en la tarea existente o crear una tarea *Instalar actualizaciones de Windows Update*.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia de uso de Kaspersky Security Center Cloud Console y el modo de funcionamiento de Kaspersky Security Center Cloud Console.

Escenario: Actualización de software de terceros

En esta sección, se describe un escenario para actualizar el software de terceros instalado en los dispositivos cliente. El software de terceros incluye aplicaciones de Microsoft y otros proveedores de software. Las actualizaciones para las aplicaciones de Microsoft se obtienen a través del servicio Windows Update.

Etapas

El proceso para actualizar aplicaciones de terceros se divide en etapas:

1. **Buscar las actualizaciones requeridas**

   Para buscar las actualizaciones que se requieren para el software de terceros de los dispositivos administrados, ejecute la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, Kaspersky Security Center Cloud Console recibe las listas de vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos que especificó en las propiedades de la tarea.

   La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente con el asistente de inicio rápido del Servidor de administración. Si no ejecutó el asistente, cree la tarea o ejecute el asistente de inicio rápido ahora.

Instrucciones:

- Creación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
- Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

2. **Analizar la lista de actualizaciones encontradas**

   Abra la lista **Actualizaciones de software** y decida qué actualizaciones se instalarán. Para obtener información detallada sobre una actualización, haga clic en el nombre de la misma en la lista. Para cada actualización de la lista, puede ver las estadísticas sobre la instalación de la actualización en los dispositivos administrados. Por ejemplo, puede ver el número de dispositivos en los que la actualización seleccionada no está instalada, se instalará o en los que la instalación de la actualización ha fallado.

   Instrucciones: Visualización de información sobre actualizaciones de software de terceros disponibles

3. **Configurar la instalación de las actualizaciones**

   Cuando Kaspersky Security Center Cloud Console recibió la lista de actualizaciones de software de terceros, puede instalarlas en los dispositivos del cliente mediante la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Instalar actualizaciones de Windows Update*. Cree una de estas tareas. Puede crearlas desde la pestaña **Tareas** o a través de la lista **Actualizaciones de software**.

   La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se utiliza para instalar actualizaciones para aplicaciones de Microsoft (incluidas las actualizaciones que proporciona el servicio Windows Update) y actualizaciones para software de otros proveedores.

   La tarea *Instalar actualizaciones de Windows Update* solo se puede utilizar para instalar actualizaciones de Windows Update.

   Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia de uso de Kaspersky Security Center Cloud Console y el modo de funcionamiento de Kaspersky Security Center Cloud Console.

   Para instalar algunas actualizaciones de software, deberá aceptar el Contrato de licencia de usuario final (EULA) para el software de instalación. Si rechaza el EULA, la actualización de software no se instalará.

   Instrucciones:

   - Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades
   - Crear la tarea Instalar actualizaciones de Windows Update
   - Ver información sobre las actualizaciones disponibles para el software de terceros

4. **Programar las tareas**

   Para asegurarse de que la lista de actualizaciones siempre esté actualizada, defina una programación que haga que la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecute automáticamente de tanto en tanto. La frecuencia predeterminada es una vez a la semana.

   Si ha creado la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede programarla para que se ejecute con la misma frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas* o con menos frecuencia. Cuando programe la tarea *Instalar actualizaciones de Windows Update*, tenga en cuenta que para esta tarea debe definir la lista de actualizaciones cada vez antes de iniciar esta tarea.

   Cuando programe las tareas, asegúrese de que las tareas para reparar vulnerabilidades se inicien después de que finalice la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

   Instrucciones: configuración general de la tarea

5. **Aprobar y rechazar actualizaciones de software (opcional)**

   Si ha creado la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede especificar reglas para la instalación de actualizaciones en las propiedades de la tarea. Si ha creado la tarea *Instalar actualizaciones de Windows Update*, omita este paso.

Para cada regla, puede definir las actualizaciones que se instalarán según el estado de la actualización (*Sin definir*, *Aprobada* o *Rechazada*). Si crea una tarea específica para sus servidores, por ejemplo, podría definir una regla que únicamente permita la instalación de actualizaciones que provengan de Windows Update y que tengan el estado *Aprobada*. Tras ello, podría asignar manualmente el estado *Aprobada* a las actualizaciones que desee instalar. Las actualizaciones de Windows Update que tengan el estado *Sin definir* o el estado *Rechazada* no se instalarán en los servidores especificados en la tarea.

De forma predeterminada, las actualizaciones de software descargadas tienen el estado *Sin definir*. Puede cambiar el estado a *Aprobada* o *Rechazada* en la lista **Actualizaciones de software** (**Operaciones** → **Administración de parches** → **Actualizaciones de software**).

Instrucciones: Aprobar y rechazar actualizaciones de software de terceros

6. **Ejecutar una tarea de instalación de actualizaciones**

   Inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o *Instalar actualizaciones de Windows Update*. Al hacerlo, se descargarán las actualizaciones y se las instalará en los dispositivos administrados. Cuando se complete la tarea ejecutada, verifique que su estado en la lista de tareas sea *Completada correctamente*.

   Instrucciones: inicio de una tarea manualmente

7. **Crear el informe sobre los resultados de la instalación de actualizaciones de software de terceros (opcional)**

   Para garantizar que se cree la tarea y se instalen las actualizaciones, cree el **Informe sobre los resultados de la instalación de actualizaciones de software de otros fabricantes** y vea las estadísticas detalladas sobre la instalación de la actualización en este informe.

   Instrucciones: Generar y ver un informe

Instalación de actualizaciones para el software de terceros

Para instalar actualizaciones para software de terceros en sus dispositivos administrados, debe crear y ejecutar alguna de las siguientes tareas:

- *Instalar actualizaciones requeridas y reparar vulnerabilidades*

  Utilice esta tarea para instalar actualizaciones de Windows Update proporcionadas por Microsoft o actualizaciones para productos de otros proveedores.

- *Instalar actualizaciones de Windows Update*

  Puede utilizar esta tarea solo para instalar actualizaciones de Windows Update.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia de uso de Kaspersky Security Center Cloud Console y el modo de funcionamiento de Kaspersky Security Center Cloud Console.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedírsele al usuario que la cierre.

Como alternativa, para crear una tarea que instale las actualizaciones requeridas, puede optar por estos métodos:

- Abra la lista de actualizaciones y elija las actualizaciones que se deban instalar.

  Como resultado, se creará una nueva tarea para instalar las actualizaciones seleccionadas. Si lo prefiere, puede agregar las actualizaciones seleccionadas a una tarea existente.

- Abra el Asistente de instalación de actualizaciones.

La disponibilidad del Asistente de instalación de actualizaciones depende del modo de Kaspersky Security Center Cloud Console y de su licencia actual.

El asistente simplifica la creación y configuración de una tarea de instalación de actualizaciones y le permite excluir la creación de tareas redundantes que contienen las mismas actualizaciones para instalar.

Instalación de actualizaciones de software de terceros desde la lista de actualizaciones

Para instalar actualizaciones de software de terceros desde la lista de actualizaciones:

1. Abra una de las listas de actualizaciones:

   - Para abrir la lista general de actualizaciones, en el menú principal vaya a **Operaciones → Administración de parches → Actualizaciones de software**.
   - Para abrir la lista de actualizaciones de un dispositivo administrado, en el menú principal vaya a **Activos (dispositivos) → Dispositivos administrados → <nombre del dispositivo> → Avanzado → Actualizaciones disponibles**.
   - Para abrir la lista de actualizaciones para una aplicación específica, en el menú principal, vaya a **Operaciones → Aplicaciones de terceros → Registro de aplicaciones → <nombre de la aplicación> → Actualizaciones disponibles**.

   Aparece una lista con las actualizaciones disponibles.

2. Active las casillas de verificación ubicadas junto a las actualizaciones que desee instalar.

3. Haga clic en el botón **Instalar actualizaciones**.

   Para instalar algunas actualizaciones de software, deberá aceptar el contrato de licencia de usuario final (EULA). Si rechaza el EULA, la actualización de software no se instalará.

4. Seleccione una de las siguientes opciones:

   - **Nueva tarea**

     Se inicia el Asistente para crear nueva tarea. La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Instalar actualizaciones de Windows Update* está preseleccionada, según el modo de Kaspersky Security Center Cloud Console y su licencia actual. Siga los pasos del asistente para completar la creación de la tarea.

   - **Instalar actualización (añadir regla a tarea específica)**

     Seleccione una tarea a la que desee agregar las actualizaciones seleccionadas. Seleccione una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* tarea o una tarea *Instalar actualizaciones de Windows Update*. Si selecciona una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, una nueva regla para instalar las actualizaciones seleccionadas se añadirá automáticamente a la tarea seleccionada. Si selecciona una tarea *Instalar actualizaciones de Windows Update*, las actualizaciones seleccionadas se añadirán a las propiedades de la tarea.

     Se abrirá la ventana de propiedades de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

Si optó por crear una tarea, se la creará y se la agregará a la lista de tareas disponible en **Activos (dispositivos) → Tareas**. Si optó por agregar las actualizaciones a una tarea existente, se agregarán las actualizaciones a las propiedades de la tarea que haya elegido.

Para instalar las actualizaciones para el software de terceros, inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Instalar actualizaciones de Windows Update*. Puede iniciar cualquiera de estas dos tareas de forma manual o, si lo prefiere, puede configurar una programación en las propiedades de la tarea que desee iniciar. Si elige configurar una programación, asegúrese de que la tarea de instalación de actualizaciones se ejecute luego de que finalice la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

Instalación de actualizaciones de software de terceros mediante el Asistente de instalación de actualizaciones

La disponibilidad de esta función depende del modo de Kaspersky Security Center Cloud Console y su licencia actual.

Para crear una tarea para instalar actualizaciones de software de terceros utilizando el Asistente de instalación de actualizaciones:

1. En el menú principal, vaya a **Operaciones → Administración de parches → Actualizaciones de software**.

   Aparece una lista con las actualizaciones disponibles.

2. Active la casilla de verificación ubicada junto a la actualización que desee instalar.

3. Haga clic en el botón **Ejecutar Asistente para la instalación de actualizaciones**.

   Se inicia el Asistente de instalación de actualizaciones. En la página **Seleccionar la tarea de instalación de actualizaciones**, verá una lista con las tareas existentes de los siguientes tipos:

   - *Instalar actualizaciones requeridas y reparar vulnerabilidades*
   - *Instalar actualizaciones de Windows Update*
   - *Reparar vulnerabilidades*

   No puede modificar las tareas de los dos últimos tipos para instalar nuevas actualizaciones. Para instalar nuevas actualizaciones, solo puede utilizar las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

4. Si desea que el asistente muestre solo las tareas que instalan la actualización que ha seleccionado, active la opción **Mostrar solo las tareas que instalan esta actualización**.

5. Elija lo que desea hacer:

   - Para iniciar una tarea, marque la casilla ubicada junto al nombre de la tarea en cuestión y haga clic en el botón **Iniciar**.
   - Para agregar una nueva regla a una tarea existente, haga lo siguiente:

     a. Marque la casilla ubicada junto al nombre de la tarea en cuestión y haga clic en el botón **Añadir regla**.

     b. En la página que se abre, configure la nueva regla:

     - Regla de instalación para actualizaciones de este nivel de importancia

Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

Esta opción está deshabilitada de manera predeterminada.

- Regla de instalación para actualizaciones de este nivel de importancia según MSRC (disponible solo para las actualizaciones de Windows Update)

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción (que solo está disponible para actualizaciones de Windows Update) está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

  Esta opción está deshabilitada de manera predeterminada.

- Regla de instalación para las actualizaciones según este proveedor (disponible solo para las actualizaciones de aplicaciones de terceros)

  Esta opción solo está disponible para actualizaciones de aplicaciones de terceros. Kaspersky Security Center Cloud Console instala solo las actualizaciones relacionadas con las aplicaciones del mismo proveedor que la actualización seleccionada. No se instalarán ni actualizaciones rechazadas ni actualizaciones para software de otros proveedores.

  Esta opción está deshabilitada de manera predeterminada.

- **Regla de instalación para las actualizaciones de tipo**
- **Regla de instalación para la actualización seleccionada**
- Aprobar actualizaciones seleccionadas

  Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

  Esta opción está deshabilitada de manera predeterminada.

- Instalar automáticamente todas las actualizaciones anteriores de la aplicación que se requieren para instalar las actualizaciones seleccionadas

Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

Esta opción está habilitada de manera predeterminada.

c. Haga clic en el botón **Añadir**.

- Para crear una tarea:

  a. Haga clic en el botón **Nueva tarea**.

  b. En la página que se abre, configure la nueva regla:

  - Regla de instalación para actualizaciones de este nivel de importancia

    Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

    Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

    Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

    Esta opción está deshabilitada de manera predeterminada.

  - Regla de instalación para actualizaciones de este nivel de importancia según MSRC (disponible solo para las actualizaciones de Windows Update)

    Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

    Si esta opción (que solo está disponible para actualizaciones de Windows Update) está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

    Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

    Esta opción está deshabilitada de manera predeterminada.

  - Regla de instalación para las actualizaciones según este proveedor (disponible solo para las actualizaciones de aplicaciones de terceros)

Esta opción solo está disponible para actualizaciones de aplicaciones de terceros. Kaspersky Security Center Cloud Console instala solo las actualizaciones relacionadas con las aplicaciones del mismo proveedor que la actualización seleccionada. No se instalarán ni actualizaciones rechazadas ni actualizaciones para software de otros proveedores.

Esta opción está deshabilitada de manera predeterminada.

- **Regla de instalación para las actualizaciones de tipo**
- **Regla de instalación para la actualización seleccionada**
- Aprobar actualizaciones seleccionadas

  Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

  Esta opción está deshabilitada de manera predeterminada.

- Instalar automáticamente todas las actualizaciones anteriores de la aplicación que se requieren para instalar las actualizaciones seleccionadas

  Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

  Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

  A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

  Esta opción está habilitada de manera predeterminada.

c. Haga clic en el botón **Añadir**.

Si ha elegido iniciar una tarea, puede cerrar el asistente. La tarea se completará en segundo plano. No se requieren más acciones.

Si optó por agregar una regla a una tarea existente, se abrirá la ventana de propiedades de la tarea. Encontrará la nueva regla en las propiedades de la tarea. Si lo desea, vea y modifique la regla u otros ajustes de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

Si eligió crear una tarea, siga creando la tarea en el Asistente para crear nueva tarea. La nueva regla que añadió en el Asistente de instalación de actualizaciones se muestra en el Asistente para crear nueva tarea. Cuando completa el Asistente para crear nueva tarea, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se añade a la lista de tareas.

Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas

A través de la tarea Buscar vulnerabilidades y actualizaciones requeridas, Kaspersky Security Center Cloud Console recibe las listas de vulnerabilidades detectadas y las actualizaciones requeridas para el software de terceros instalado en los dispositivos administrados.

La tarea Buscar vulnerabilidades y actualizaciones requeridas se crea automáticamente cuando se ejecuta el asistente de inicio rápido. Si no ejecutó el asistente, puede crear la tarea manualmente.

Para crear la tarea Buscar vulnerabilidades y actualizaciones requeridas, realice lo siguiente:

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 Cloud Console, seleccione el tipo de tarea **Buscar vulnerabilidades y actualizaciones requeridas**.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Seleccione los dispositivos a los que se asignará la tarea.
6. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.
7. Haga clic en el botón **Crear**.

   Se crea la tarea y se la agrega a la lista de tareas.
8. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.
9. En la ventana de propiedades de la tarea, configure los ajustes generales de la tarea.
10. En la pestaña **Configuración de la aplicación**, defina los siguientes ajustes:

    - **Buscar vulnerabilidades y actualizaciones en la lista de Microsoft**

      Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center Cloud Console utiliza la información sobre las actualizaciones de Microsoft aplicables desde el origen de actualizaciones de Microsoft, las cuales están disponibles en este momento.

      Podría deshabilitar esta opción si, por ejemplo, ha creado tareas diferentes (con configuraciones diferentes) para las actualizaciones de Microsoft y para las actualizaciones de aplicaciones de terceros.

      Esta opción está habilitada de manera predeterminada.

      La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

    - **Conectar al servidor de actualizaciones para actualizar los datos**

El Agente de Windows Update del dispositivo administrado se conectará al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como orígenes de actualizaciones de Microsoft:

- Servidor de administración de Kaspersky Security Center Cloud Console (consulte la configuración de la directiva del Agente de red)
- Un servidor Windows Server con Microsoft Windows Server Update Services (WSUS) que se encuentre instalado en la red de su organización
- Los servidores de actualizaciones de Microsoft

Cuando esta opción está habilitada, el Agente de Windows Update del dispositivo administrado se conecta al origen de actualizaciones de Microsoft para obtener información actualizada sobre las actualizaciones de Microsoft Windows aplicables.

Cuando esta opción está desactivada, el Agente de Windows Update del dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que el origen de actualizaciones de Microsoft brindó en un momento anterior.

Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Podría deshabilitar esta opción si ha configurado un esquema de conexión periódica a este origen en otra tarea o en la sección **Vulnerabilidades y actualizaciones de software** de las propiedades de la directiva del Agente de red. Si no quiere deshabilitar esta opción, para intentar que el Servidor de administración no se sobrecargue, modifique la programación de la tarea para que se la inicie en un punto aleatorio de un intervalo de 360 minutos.

Esta opción está habilitada de manera predeterminada.

El modo de obtener las actualizaciones deriva de combinar las siguientes opciones de configuración de la directiva del Agente de red:

- El Agente de Windows Update en un dispositivo administrado se conecta al Servidor de actualizaciones para obtener actualizaciones solo si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está activada en las propiedades de la tarea *Buscar vulnerabilidades y actualizaciones requeridas* y la opción de **Modo de búsqueda de Windows Update** está configurada como **Activo** en la configuración de la directiva del Agente de red.
- Si no necesita el Agente de red para iniciar una conexión al origen de actualizaciones de Microsoft Windows y descargar actualizaciones al realizar la tarea *Análisis de vulnerabilidades*, puede establecer la opción de **Modo de búsqueda de Windows Update** en **Pasivo**, mientras que la opción **Conectar al servidor de actualizaciones para actualizar los datos** debe permanecer activado. Esto le permite ahorrar recursos y usar las actualizaciones de Windows recibidas anteriormente para buscar vulnerabilidades. Puede usar el modo pasivo si configura la recepción de actualizaciones de Microsoft Windows de otra manera. Si la recepción de actualizaciones de Microsoft Windows no está configurada de otra manera, no establezca la opción del **Modo de búsqueda de Windows Update** en **Pasivo**, ya que nunca recibirá información sobre las actualizaciones.
- Independientemente del estado de la opción **Conectar al servidor de actualizaciones para actualizar los datos** (activada o desactivada), si la opción **Desactivado** está marcada en **Modo de búsqueda de Windows Update**, Kaspersky Security Center Cloud Console no solicita ninguna información sobre actualizaciones.

- Buscar vulnerabilidades y actualizaciones de terceros en la lista de Kaspersky

Si esta opción está activada, Kaspersky Security Center Cloud Console busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especificar rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky determina el alcance de la lista de aplicaciones de terceros compatibles.

Si esta opción está desactivada, Kaspersky Security Center Cloud Console no busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros. Puede que quiera deshabilitar esta opción si utiliza tareas diferentes, con configuraciones diferentes, para las actualizaciones de Microsoft Windows y para las actualizaciones de aplicaciones de terceros.

Esta opción está habilitada de manera predeterminada.

- Especifique rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos

  Las carpetas en las que Kaspersky Security Center Cloud Console busca aplicaciones de terceros que requieren una reparación de vulnerabilidad y una instalación de actualización. Puede utilizar variables del sistema.

  Especifique las carpetas en las que se instalan las aplicaciones. De forma predeterminada, la lista está vacía.

- Activar diagnóstico avanzado

  Si esta función está activada, el Agente de red escribe los rastreos incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center Cloud Console. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está desactivada, el Agente de red escribe rastros de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center Cloud Console. No se guardará ningún otro dato de seguimiento.

  No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está deshabilitada de manera predeterminada.

- Tamaño máximo, en MB, de los archivos de diagnóstico avanzado

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

11. Haga clic en el botón **Guardar**.

La tarea queda creada y configurada.

Si el resultado de la tarea contiene una advertencia sobre el error 0x80240033, deberá recurrir al Registro de Windows para resolver el inconveniente. El error indica lo siguiente: "Error del Agente de Windows Update 80240033 ("No se pudieron descargar los términos de licencia.")".

Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente cuando se ejecuta el asistente de inicio rápido. Si no ejecutó el asistente, puede crear la tarea manualmente.

A continuación, se describen los ajustes que puede configurar para la tarea *Buscar vulnerabilidades y actualizaciones requeridas* (junto con sus ajustes generales) ya sea al momento de crear la tarea o, si la tarea ya existe, a través de sus propiedades:

- **Buscar vulnerabilidades y actualizaciones en la lista de Microsoft**

  Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center Cloud Console utiliza la información sobre las actualizaciones de Microsoft aplicables desde el origen de actualizaciones de Microsoft, las cuales están disponibles en este momento.

  Podría deshabilitar esta opción si, por ejemplo, ha creado tareas diferentes (con configuraciones diferentes) para las actualizaciones de Microsoft y para las actualizaciones de aplicaciones de terceros.

  Esta opción está habilitada de manera predeterminada.

  La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

- **Conectar al servidor de actualizaciones para actualizar los datos**

El Agente de Windows Update del dispositivo administrado se conectará al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como orígenes de actualizaciones de Microsoft:

- Servidor de administración de Kaspersky Security Center Cloud Console (consulte la configuración de la directiva del Agente de red)
- Un servidor Windows Server con Microsoft Windows Server Update Services (WSUS) que se encuentre instalado en la red de su organización
- Los servidores de actualizaciones de Microsoft

Cuando esta opción está habilitada, el Agente de Windows Update del dispositivo administrado se conecta al origen de actualizaciones de Microsoft para obtener información actualizada sobre las actualizaciones de Microsoft Windows aplicables.

Cuando esta opción está desactivada, el Agente de Windows Update del dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que el origen de actualizaciones de Microsoft brindó en un momento anterior.

Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Podría deshabilitar esta opción si ha configurado un esquema de conexión periódica a este origen en otra tarea o en la sección **Vulnerabilidades y actualizaciones de software** de las propiedades de la directiva del Agente de red. Si no quiere deshabilitar esta opción, para intentar que el Servidor de administración no se sobrecargue, modifique la programación de la tarea para que se la inicie en un punto aleatorio de un intervalo de 360 minutos.

Esta opción está habilitada de manera predeterminada.

El modo de obtener las actualizaciones deriva de combinar las siguientes opciones de configuración de la directiva del Agente de red:

- El Agente de Windows Update en un dispositivo administrado se conecta al Servidor de actualizaciones para obtener actualizaciones solo si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está activada en las propiedades de la tarea *Buscar vulnerabilidades y actualizaciones requeridas* y la opción de **Modo de búsqueda de Windows Update** está configurada como **Activo** en la configuración de la directiva del Agente de red.
- Si no necesita el Agente de red para iniciar una conexión al origen de actualizaciones de Microsoft Windows y descargar actualizaciones al realizar la tarea *Análisis de vulnerabilidades*, puede establecer la opción de **Modo de búsqueda de Windows Update** en **Pasivo**, mientras que la opción **Conectar al servidor de actualizaciones para actualizar los datos** debe permanecer activado. Esto le permite ahorrar recursos y usar las actualizaciones de Windows recibidas anteriormente para buscar vulnerabilidades. Puede usar el modo pasivo si configura la recepción de actualizaciones de Microsoft Windows de otra manera. Si la recepción de actualizaciones de Microsoft Windows no está configurada de otra manera, no establezca la opción del **Modo de búsqueda de Windows Update** en **Pasivo**, ya que nunca recibirá información sobre las actualizaciones.
- Independientemente del estado de la opción **Conectar al servidor de actualizaciones para actualizar los datos** (activada o desactivada), si la opción **Desactivado** está marcada en **Modo de búsqueda de Windows Update**, Kaspersky Security Center Cloud Console no solicita ninguna información sobre actualizaciones.

- Buscar vulnerabilidades y actualizaciones de terceros en la lista de Kaspersky

Si esta opción está activada, Kaspersky Security Center Cloud Console busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especificar rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky determina el alcance de la lista de aplicaciones de terceros compatibles.

Si esta opción está desactivada, Kaspersky Security Center Cloud Console no busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros. Puede que quiera deshabilitar esta opción si utiliza tareas diferentes, con configuraciones diferentes, para las actualizaciones de Microsoft Windows y para las actualizaciones de aplicaciones de terceros.

Esta opción está habilitada de manera predeterminada.

- **Especifique rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**

  Las carpetas en las que Kaspersky Security Center Cloud Console busca aplicaciones de terceros que requieren una reparación de vulnerabilidad y una instalación de actualización. Puede utilizar variables del sistema.

  Especifique las carpetas en las que se instalan las aplicaciones. De forma predeterminada, la lista está vacía.

- **Activar diagnóstico avanzado**

  Si esta función está activada, el Agente de red escribe los rastreos incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center Cloud Console. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está desactivada, el Agente de red escribe rastros de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center Cloud Console. No se guardará ningún otro dato de seguimiento.

  No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está deshabilitada de manera predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

Recomendaciones para programar la tarea

Al programar la tarea *Buscar vulnerabilidades y actualizaciones requeridas*, asegúrese de que las opciones **Ejecutar tareas no realizadas** y **Usar el retraso aleatorio automáticamente para el inicio de la tarea** estén habilitadas.

De forma predeterminada, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* está configurada para iniciarse de forma manual. Si las reglas del espacio de trabajo de la organización estipulan que todos los dispositivos se apagan a esa hora, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecutará una vez que los dispositivos se enciendan nuevamente, es decir, la mañana siguiente. Esto puede ser inconveniente porque los análisis de vulnerabilidades pueden hacer que aumente la carga en los subsistemas de disco y CPU. Debe buscar que la programación de la tarea se adecue a las reglas dispuestas por su organización.

Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades

La disponibilidad de la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* depende del modo de consola de Kaspersky Security Center Cloud Console y de su licencia actual.

Utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para aplicar actualizaciones y reparar vulnerabilidades en las aplicaciones de terceros (incluidas las de Microsoft) instaladas en los dispositivos administrados. Esta tarea le permite instalar múltiples actualizaciones y corregir múltiples vulnerabilidades de acuerdo con ciertas reglas.

Si desea usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar actualizaciones o reparar vulnerabilidades, realice alguna de las siguientes acciones:

- Ejecute el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.
- Cree una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Agregue una regla de instalación de actualizaciones a una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* existente.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia de uso de Kaspersky Security Center Cloud Console y el modo de funcionamiento de Kaspersky Security Center Cloud Console.

Para crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades:

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 Cloud Console, seleccione el tipo de tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Seleccione los dispositivos a los que se asignará la tarea.
6. Defina las reglas de instalación de actualizaciones y luego configure los siguientes ajustes:
   - **Iniciar la instalación al reiniciar o apagar el dispositivo**

Si esta opción está habilitada, las actualizaciones se instalarán en el momento en el que los dispositivos se reinicien o se apaguen. De lo contrario, las actualizaciones se instalarán siguiendo la programación que se defina.

Utilice esta opción si la instalación de las actualizaciones podría afectar el rendimiento de los dispositivos.

Esta opción está deshabilitada de manera predeterminada.

- Instalar los componentes generales del sistema necesarios

  Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Por ejemplo, estos requisitos previos pueden ser actualizaciones del sistema operativo.

  Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

  Esta opción está deshabilitada de manera predeterminada.

- Autorizar la instalación de las nuevas versiones de la aplicación durante las actualizaciones

  Si esta opción está habilitada, las actualizaciones podrán cambiar la versión del software actualizado por una más reciente.

  Si esta opción está deshabilitada, los cambios de versión no estarán permitidos. Para instalar una versión más reciente de una aplicación, deberá usar una tarea diferente o proceder en forma manual. Podría usar esta opción si, por ejemplo, desea evaluar el cambio de versión en una infraestructura de prueba o si sabe que la versión más reciente no es compatible con la infraestructura de su empresa.

  Esta opción está habilitada de manera predeterminada.

  Los cambios de versión pueden ocasionar problemas de funcionamiento en las aplicaciones dependientes instaladas en los dispositivos cliente.

- Descargar actualizaciones en el dispositivo sin instalarlas

  Si esta opción está habilitada, la aplicación descargará las actualizaciones disponibles en los dispositivos, pero no las instalará automáticamente. Podrá instalar las actualizaciones descargadas manualmente.

  Las actualizaciones de Microsoft se descargan en el sistema de almacenamiento de Windows. Las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft) se descargan en la carpeta especificada en el campo **Descargar actualizaciones en**.

  Si esta opción está deshabilitada, las actualizaciones se instalarán en los dispositivos automáticamente.

  Esta opción está deshabilitada de manera predeterminada.

- Descargar actualizaciones en

  Esta carpeta se utiliza para descargar las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft).

- Activar diagnóstico avanzado

Si esta función está activada, el Agente de red escribe los rastreos incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center Cloud Console. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

Si esta función está desactivada, el Agente de red escribe rastros de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center Cloud Console. No se guardará ningún otro dato de seguimiento.

No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

Esta opción está deshabilitada de manera predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

7. Especifique la configuración 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)**

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.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está habilitada de manera predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Tiempo de espera antes del cierre forzado de aplicaciones en sesiones bloqueadas (min)**

  Las aplicaciones se cerrarán por la fuerza cuando el dispositivo del usuario se bloquee (sea manualmente o en forma automática tras un tiempo de inactividad).

  Si esta opción está habilitada, las aplicaciones del dispositivo bloqueado se cerrarán por la fuerza luego de transcurra el intervalo especificado en el campo de entrada.

  Si esta opción está deshabilitada, las aplicaciones del dispositivo bloqueado no se cerrarán.

  Esta opción está deshabilitada de manera predeterminada.

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.

Si el resultado de la tarea contiene una advertencia sobre el error 0x80240033, deberá recurrir al Registro de Windows para resolver el inconveniente. El error indica lo siguiente: "Error del Agente de Windows Update 80240033 ("No se pudieron descargar los términos de licencia.")".

Agregar reglas de instalación de actualizaciones

La disponibilidad de esta función depende del modo de Kaspersky Security Center Cloud Console y su licencia actual.

Si desea utilizar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar actualizaciones de software o reparar vulnerabilidades en sus aplicaciones, debe definir reglas de instalación de actualizaciones. Estas reglas determinan qué actualizaciones se deben instalar y qué vulnerabilidades se deben reparar.

La configuración exacta depende de si la regla se crea para todas las actualizaciones, para actualizaciones de Windows Update o para actualizaciones publicadas para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky y Microsoft). Cuando agregue una regla para actualizaciones de Windows Update o para actualizaciones de aplicaciones de terceros, podrá seleccionar las aplicaciones específicas (y las versiones puntuales de esas aplicaciones) para las que quiera instalar actualizaciones. Cuando agregue una regla para todas las actualizaciones, podrá seleccionar las actualizaciones específicas que quiera instalar y las vulnerabilidades puntuales que quiera reparar mediante la instalación de actualizaciones.

Para agregar una regla de instalación de actualizaciones, puede optar por cualquiera de estos métodos:

- Al añadir una regla mientras crea una nueva tarea Instalar actualizaciones requeridas y reparar vulnerabilidades.
- Agregue la regla en la pestaña **Configuración de la aplicación** de la ventana de propiedades de una tarea de *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Mediante el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.

Para agregar una nueva regla para todas las actualizaciones:

1. Haga clic en el botón **Añadir**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Next**.

2. En la página **Tipo de regla**, seleccione **Regla para todas las actualizaciones**.

3. En la página **Criterios generales**, use las listas desplegables para definir los siguientes ajustes:

   - **Conjunto de actualizaciones para instalar**

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:
     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - **Reparar vulnerabilidades con un nivel de gravedad igual o mayor que**

Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

Esta opción está deshabilitada de manera predeterminada.

4. En la página **Actualizaciones**, seleccione las actualizaciones que se instalarán:

- **Instalar todas las actualizaciones pertinentes**

  Instalar todas las actualizaciones de software que cumplan con los criterios especificados en la página de **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

- **Instalar solo las actualizaciones de la lista**

  Se instalarán únicamente las actualizaciones de software que seleccione manualmente en la lista. La lista contiene todas las actualizaciones de software disponibles.

  Existen situaciones en las que querrá elegir manualmente las actualizaciones que se instalarán: podría suceder, por ejemplo, que quiera evaluar ciertas actualizaciones en un entorno de prueba, que quiera actualizar solo las aplicaciones que considere importantes o que necesite actualizar solo algunas aplicaciones puntuales.

- **Instalar automáticamente todas las actualizaciones anteriores de la aplicación que se requieren para instalar las actualizaciones seleccionadas**

  Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

  Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

  A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

  Esta opción está habilitada de manera predeterminada.

5. En la página **Vulnerabilidades**, seleccione las vulnerabilidades que se repararán al instalar las actualizaciones seleccionadas:

- **Reparar todas las vulnerabilidades que coinciden con otros criterios**

  Reparar todas las vulnerabilidades que cumplan con los criterios especificados en la página de **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

- Reparar solo las vulnerabilidades de la lista

  Se repararán únicamente las vulnerabilidades que seleccione manualmente en la lista. La lista contiene todas las vulnerabilidades detectadas.

  Existen situaciones en las que querrá elegir manualmente las vulnerabilidades que se repararán: podría suceder, por ejemplo, que quiera verificar en un entorno de prueba que las vulnerabilidades se puedan reparar, que quiera reparar las vulnerabilidades solo en las aplicaciones que considere importantes o que prefiera reparar las vulnerabilidades solo en ciertas aplicaciones puntuales.

6. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Una vez que el Asistente de creación de reglas finaliza su operación, la nueva regla se añade y se muestra en el campo del Asistente para crear nueva tarea.

Para agregar una nueva regla para actualizaciones de Windows Update:

1. Haga clic en el botón **Añadir**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Next**.

2. En la página **Tipo de regla**, seleccione **Regla para Windows Update**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - Reparar vulnerabilidades con un nivel de gravedad igual o mayor que

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

     Esta opción está deshabilitada de manera predeterminada.

   - Reparar vulnerabilidades con un nivel de gravedad MSRC igual o mayor que

Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

Esta opción está deshabilitada de manera predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Categorías de actualizaciones**, seleccione las categorías de actualizaciones que se instalarán. Las categorías son las mismas que se usan en el Catálogo de Microsoft Update. Por defecto, están seleccionadas todas las categorías.

6. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Una vez que el Asistente de creación de reglas finaliza su operación, la nueva regla se añade y se muestra en el campo del Asistente para crear nueva tarea.

Para agregar una nueva regla para actualizaciones de aplicaciones de terceros:

1. Haga clic en el botón **Añadir**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Next**.

2. En la página **Tipo de regla**, seleccione **Regla para actualizaciones de terceros**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - Reparar vulnerabilidades con un nivel de gravedad igual o mayor que

Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

Esta opción está deshabilitada de manera predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección Configuración de la ventana de propiedades de la tarea creada.

Una vez que el Asistente de creación de reglas finaliza su operación, la nueva regla se añade y se muestra en el campo del Asistente para crear nueva tarea.

Crear la tarea Instalar actualizaciones de Windows Update

La tarea Instalar actualizaciones de Windows Update le permite instalar actualizaciones de software proporcionadas por el servicio de Windows Update en dispositivos cliente.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia de uso de Kaspersky Security Center Cloud Console y el modo de funcionamiento de Kaspersky Security Center Cloud Console.

Para crear la tarea "Instalar actualizaciones de Windows Update":

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 Cloud Console, seleccione el tipo de tarea **Instalar actualizaciones de Windows Update**.

4. Escriba un nombre para la tarea que está creando.

   El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).

5. Seleccione los dispositivos a los que se asignará la tarea.

6. Haga clic en el botón **Añadir**.

   Se abre la lista de actualizaciones.

7. Seleccione las actualizaciones de Windows Update que desee instalar y, a continuación, haga clic en **Aceptar**.

8. Defina las opciones de reinicio del sistema operativo:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o 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)**

  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.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está 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.

9. Configure los ajustes relativos a la cuenta:

- **Cuenta predeterminada**

  La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

  Esta opción está seleccionada de 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.

10. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.

11. Haga clic en el botón **Finalizar**.

    Se crea la tarea y se la agrega a la lista de tareas.

12. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

13. En la ventana de propiedades de la tarea, modifique los ajustes generales de la tarea según resulte necesario.

14. Haga clic en el botón **Guardar**.

La tarea queda creada y configurada.

Ver información sobre las actualizaciones disponibles para el software de terceros

Puede ver la lista de actualizaciones disponibles para las aplicaciones de terceros instaladas en los dispositivos cliente (incluidas las aplicaciones de Microsoft).

Para ver una lista de las actualizaciones disponibles para las aplicaciones de terceros instaladas en los dispositivos cliente,

En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Actualizaciones de software**.

Aparece una lista con las actualizaciones disponibles.

Puede aplicar un filtro para ver la lista de actualizaciones de software. Para definir el filtro, haga clic en el ícono **Filtro** ( ) ubicado en la esquina superior derecha de la lista de actualizaciones de software. También puede elegir un filtro preestablecido de la lista desplegable **Preestablecer filtros**, que se encuentra sobre la lista de vulnerabilidades de software.

Para ver las propiedades de una actualización:

1. Haga clic en el nombre de la actualización de software que sea de su interés.
2. Se abrirá la ventana de propiedades de la actualización, que consta de las siguientes pestañas con información:

- **General**

  Esta pestaña contiene los detalles generales de la actualización seleccionada:

  - Estado de aprobación de la actualización (si desea cambiar este estado, puede elegir uno diferente en la lista desplegable)
  - Categoría de Windows Server Update Services (WSUS) a la que pertenece la actualización
  - Fecha y hora en que se registró la actualización
  - Fecha y hora en que se creó la actualización
  - Nivel de importancia de la actualización
  - Requisitos de instalación impuestos por la actualización
  - Familia de aplicaciones a la que pertenece la actualización
  - Aplicación a la que corresponde la actualización
  - Número de revisión de la actualización

- **Atributos**

Esta pestaña muestra una serie de atributos que permiten buscar más información sobre la actualización seleccionada. Los atributos disponibles dependen de si la actualización fue publicada por Microsoft o por otro desarrollador.

Cuando una actualización proviene de Microsoft, la información disponible en la pestaña es la siguiente:

- Nivel de importancia asignado a la actualización por el Centro de respuestas de seguridad de Microsoft (MSRC)
- Vínculo al artículo de Microsoft Knowledge Base en el que se describe la actualización
- Vínculo al artículo del boletín de seguridad de Microsoft en el que se describe la actualización
- Identificador (id.) de la actualización

Cuando una actualización proviene de otro desarrollador, la información disponible en la pestaña es la siguiente:

- Indicador de si la actualización es un parche o un paquete de distribución completo
- Idioma de localización de la actualización
- Indicador de si la actualización se instaló de forma manual o automática
- Indicador de si la actualización se revocó tras ser instalada
- Vínculo de descarga de la actualización

- **Dispositivos**

  Esta pestaña contiene la lista de dispositivos en los que se encuentra instalada la actualización elegida.

- **Vulnerabilidades reparadas**

  Esta pestaña contiene la lista de vulnerabilidades que pueden repararse con la actualización seleccionada.

- **Cruce de actualizaciones**

  Esta pestaña muestra cualquier "cruce" que pueda existir entre las actualizaciones publicadas para una misma aplicación; en otras palabras, aquí se indica si la actualización seleccionada puede reemplazar a otras actualizaciones o si, por el contrario, puede ser reemplazada por otras. Esta información solo está disponible para actualizaciones de Microsoft.

- **Tareas para instalar esta actualización**

  Esta pestaña contiene una lista de tareas que, por su alcance, pueden usarse para instalar la actualización seleccionada. Desde aquí también se puede crear una nueva tarea de instalación remota para la actualización.

Para ver las estadísticas de instalación de una actualización:

1. Active la casilla de verificación ubicada junto a la actualización de software que sea de su interés.

2. Haga clic en el botón **Estadísticas del estado de instalación de las actualizaciones**.

   Se muestra un diagrama con los estados de instalación de la actualización. Si hace clic en un estado, se abrirá una lista con los dispositivos en los que la actualización tenga el estado seleccionado.

Puede ver información sobre las actualizaciones de software disponibles para el software de terceros (incluido el software de Microsoft) instalado en un dispositivo con Windows en particular.

Para ver una lista de las actualizaciones disponibles para el software de terceros instalado en un dispositivo administrado específico:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo sobre el que quiera información.

   Se muestra la ventana de propiedades del dispositivo seleccionado.

3. En la ventana de propiedades del dispositivo seleccionado, elija la pestaña **Avanzado**.

4. En el panel de la izquierda, elija la sección **Actualizaciones disponibles**. Si solo desea ver las actualizaciones instaladas, seleccione la opción **Mostrar las actualizaciones instaladas**.

   Se muestra la lista de actualizaciones de software de terceros disponibles para el dispositivo seleccionado.

Exportar la lista de actualizaciones de software disponibles a un archivo

Puede exportar a un archivo CSV o TXT la lista de actualizaciones disponibles para las aplicaciones de terceros (incluidas las de Microsoft) que se muestra en un momento dado. Una vez que tenga el archivo, podrá almacenarlo para fines estadísticos, enviarlo a la persona que esté a cargo de la seguridad de la información o utilizarlo para otros fines.

Para exportar a un archivo de texto la lista de actualizaciones disponibles para el software de terceros instalado en todos los dispositivos administrados:

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Actualizaciones de software**.

   La página muestra una lista de actualizaciones disponibles para el software de terceros instalado en todos los dispositivos administrados.

2. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera.

   El archivo con la lista de actualizaciones disponibles para el software de terceros, incluido el software de Microsoft, se guardará en el dispositivo que esté utilizando.

Para exportar a un archivo de texto la lista de actualizaciones disponibles para el software de terceros instalado en un dispositivo administrado específico:

1. Abra la lista de actualizaciones de software de terceros disponibles para el dispositivo administrado pertinente.

2. Seleccione las actualizaciones de software que desee exportar.

   Omita este paso si desea exportar toda la lista de actualizaciones de software.

   Si desea exportar la lista completa de actualizaciones de software, tenga en cuenta que solo se exportarán las actualizaciones que aparezcan en la página que esté viendo.

   Si desea exportar solo las actualizaciones instaladas, active la casilla de verificación **Mostrar las actualizaciones instaladas**.

3. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera.

En el dispositivo que esté utilizando, se guardará un archivo con la lista de actualizaciones disponibles para el software de terceros (incluido el software de Microsoft) instalado en el dispositivo administrado seleccionado.

Aprobar y rechazar actualizaciones de software de terceros

Al configurar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede crear una regla que exija que las actualizaciones que se deban instalar tengan un estado específico. Una regla de actualización puede permitir, por ejemplo, la instalación de estas actualizaciones:

- Solo las actualizaciones aprobadas
- Solo las actualizaciones aprobadas o sin estado definido
- Todas las actualizaciones, independientemente de su estado

Puede aprobar las actualizaciones que deban instalarse y rechazar las que no deban instalarse.

Puede usar el estado *Aprobada* para administrar la instalación de un número modesto de actualizaciones. Para instalar varias actualizaciones, utilice las reglas que puede configurar en la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Asigne el estado *Aprobada* únicamente a las actualizaciones que no cumplan con los criterios indicados en las reglas. Aprobar un gran número de actualizaciones en forma manual afecta el rendimiento del Servidor de administración y puede, incluso, hacer que se sobrecargue.

Para aprobar o rechazar una o más actualizaciones:

1. En el menú principal, vaya a **Operaciones → Administración de parches → Actualizaciones de software**.

   Aparece una lista con las actualizaciones disponibles.

2. Seleccione las actualizaciones que desee aprobar o rechazar.

3. Haga clic en **Aprobar** para aprobar las actualizaciones seleccionadas o en **Rechazar** para rechazarlas.

   El valor predeterminado es *Sin definir*.

Los estados de las actualizaciones seleccionadas cambian a los que ha elegido.

Como alternativa, puede cambiar el estado de aprobación en las propiedades de una actualización específica.

Para aprobar o rechazar una actualización desde sus propiedades:

1. En el menú principal, vaya a **Operaciones → Administración de parches → Actualizaciones de software**.

   Aparece una lista con las actualizaciones disponibles.

2. Haga clic en el nombre de la actualización que desee aprobar o rechazar.

   Se abre la ventana de propiedades de la actualización.

3. En la sección **General**, cambie la opción **Estado de aprobación de la actualización** para elegir el estado de la actualización. Puede seleccionar los estados *Aprobada*, *Rechazada* o *Sin definir*.

4. Haga clic en el botón **Guardar** para guardar los cambios.

El estado de la actualización seleccionada cambia al que ha elegido.

Si asigna el estado **Rechazada** a las actualizaciones de software de un tercero, estas no se instalarán en los dispositivos a los que estén asignadas, pero que aún no las hayan recibido. Las actualizaciones no se borrarán de los dispositivos en los que ya se encuentren instaladas. Si necesita eliminar estas actualizaciones, hágalo manualmente en forma local.

Actualización automática de aplicaciones de terceros

Algunas aplicaciones de terceros se pueden actualizar automáticamente. Quien determina si una aplicación es compatible con la función de actualización automática es su desarrollador o proveedor. Si una aplicación de terceros instalada en un dispositivo administrado se puede actualizar automáticamente, podrá configurar el ajuste de actualización automática en las propiedades de esa aplicación. Luego de que modifique este ajuste, las instancias del Agente de red implementarán el nuevo valor en cada dispositivo administrado que tenga instalada esa aplicación.

La configuración de actualización automática es independiente de los otros objetos y ajustes de la función Administración de vulnerabilidades y parches. Este ajuste, por ejemplo, no se ve afectado por los estados de aprobación de las actualizaciones ni por las distintas tareas de instalación de actualizaciones, como *Instalar actualizaciones requeridas y reparar vulnerabilidades*, *Instalar actualizaciones de Windows Update* y *Reparar vulnerabilidades*.

Para configurar el ajuste de actualización automática para una aplicación creada por un tercero:

1. En el menú principal, vaya a **Operaciones → Aplicaciones de terceros → Registro de aplicaciones**.

2. Haga clic en el nombre de la aplicación para la que desee modificar el ajuste de actualización automática.

   Puede usar la columna **Estado de las actualizaciones automáticas** para filtrar la lista y simplificar la búsqueda.

   Se abrirá la ventana de propiedades de la aplicación.

3. En la sección **General**, seleccione un valor para el siguiente ajuste:

   Estado de las actualizaciones automáticas

Seleccione una de las siguientes opciones:

- **Sin definir**

  Se deshabilitará la función de actualización automática. Kaspersky Security Center Cloud Console instala actualizaciones de aplicaciones de terceros mediante el uso de las siguientes tareas: *Instalar actualizaciones requeridas y reparar vulnerabilidades*, *Instalar actualizaciones de Windows Update* y *Reparar vulnerabilidades*.

- **Permitido**

  Las actualizaciones que el proveedor publique para la aplicación se instalarán automáticamente en los dispositivos administrados. No se requerirá ninguna otra acción.

- **Bloqueado**

  Las actualizaciones para la aplicación no se instalarán automáticamente. Kaspersky Security Center Cloud Console instala actualizaciones de aplicaciones de terceros mediante el uso de las siguientes tareas: *Instalar actualizaciones requeridas y reparar vulnerabilidades*, *Instalar actualizaciones de Windows Update* y *Reparar vulnerabilidades*.

4. Haga clic en el botón **Guardar** para guardar los cambios.

El valor definido para el ajuste de actualización automática se implementa en la aplicación seleccionada.

Encontrar y corregir vulnerabilidades de software

Kaspersky Security Center Cloud Console detecta y corrige vulnerabilidades de software en dispositivos administrados que ejecutan los sistemas operativos de las familias Microsoft Windows. Se detectan vulnerabilidades en el sistema operativo y en el software de terceros, incluido el software de Microsoft.

La función de actualizaciones (incluido el suministro de actualizaciones de las firmas antivirus y de la base de código) y la función de KSN pueden dejar de estar disponibles en el software en el territorio de EE. UU.

Búsqueda de vulnerabilidades de software

Para buscar las vulnerabilidades de software, Kaspersky Security Center Cloud Console utiliza características de la base de datos de vulnerabilidades conocidas y de Windows Update. A la base de datos de las vulnerabilidades conocidas la crean y mantienen los especialistas de Kaspersky. Contiene distintos datos sobre cada vulnerabilidad: su descripción, su fecha de detección, su nivel de gravedad y más. Puede ver los detalles de las vulnerabilidades de software en el sitio web de Kaspersky.

Kaspersky Security Center Cloud Console utiliza la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para buscar vulnerabilidades de software.

Reparación de vulnerabilidades de software

Para corregir vulnerabilidades de software, Kaspersky Security Center Cloud Console utiliza actualizaciones de software emitidas por los proveedores de software. Puede ver la lista de vulnerabilidades de software en cualquier momento. Los metadatos de las actualizaciones de software se descargan automáticamente en el repositorio del Servidor de administración y en los repositorios de los puntos de distribución como resultado de la ejecución de la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*. Puede crear esta tarea con el asistente de inicio rápido de Kaspersky Security Center Cloud Console o manualmente.

Las actualizaciones de software que se utilizan para corregir vulnerabilidades pueden representarse como paquetes de distribución completos o como parches. Las actualizaciones de software diseñadas para corregir vulnerabilidades de software se denominan *reparaciones*. En Kaspersky Security Center Cloud Console, usted corrige las vulnerabilidades mediante las *correcciones recomendadas*. Las correcciones recomendadas son actualizaciones de software que los especialistas de Kaspersky recomiendan instalar.

Dependiendo del modo de Kaspersky Security Center Cloud Console y su licencia actual, puede usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* tarea o la tarea *Reparar vulnerabilidades* para reparar vulnerabilidades de software.

La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* instala las correcciones recomendadas para corregir automáticamente múltiples vulnerabilidades. Si utiliza esta tarea, puede configurar manualmente ciertas reglas para la reparación de múltiples vulnerabilidades.

Mediante la tarea *Reparar vulnerabilidades*, puede instalar las correcciones recomendadas para corregir vulnerabilidades del software de Microsoft.

Por razones de seguridad, las tecnologías de Kaspersky analizan automáticamente en busca de malware cualquier actualización de software de terceros que instale mediante la función Administración de vulnerabilidades y parches. Estas tecnologías se utilizan para la verificación automática de archivos e incluyen análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno de pruebas y aprendizaje automático.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. Además, los expertos de Kaspersky no buscan vulnerabilidades (conocidas o desconocidas) ni funciones no documentadas en dichas actualizaciones, ni realizan otros tipos de análisis de las actualizaciones distintos a los especificados en el párrafo anterior.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia de uso de Kaspersky Security Center Cloud Console y el modo de funcionamiento de Kaspersky Security Center Cloud Console.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedírsele al usuario que la cierre.

Para reparar algunas vulnerabilidades de software, deberá aceptar un contrato de licencia de usuario final (EULA) que lo faculte a instalar el software. Si se le solicita aceptar el EULA, hágalo. Si rechaza el EULA, la vulnerabilidad del software no se repara.

La información sobre cada vulnerabilidad reparada se almacena en el Servidor de administración durante 90 días. Transcurrido este plazo, se la elimina automáticamente.

Reparación de vulnerabilidades de software

Una vez que ha obtenido la lista de vulnerabilidades de software, puede reparar las vulnerabilidades de software que estén presentes en los dispositivos Windows administrados. Para reparar vulnerabilidades de software en el sistema operativo y en las aplicaciones creadas por terceros (incluido Microsoft), cree y ejecute la tarea *Reparar vulnerabilidades* o la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia de uso de Kaspersky Security Center Cloud Console y el modo de funcionamiento de Kaspersky Security Center Cloud Console.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedírsele al usuario que la cierre.

Como alternativa, para crear una tarea para reparar vulnerabilidades de software, puede optar por estas vías:

- Abra la lista de vulnerabilidades y seleccione las vulnerabilidades que desee reparar.

  Como resultado, se creará una nueva tarea para reparar esas vulnerabilidades de software. Si lo prefiere, puede agregar las vulnerabilidades seleccionadas a una tarea existente.

- Abra el Asistente de reparación de vulnerabilidades.

  La disponibilidad de esta función depende del modo de Kaspersky Security Center Cloud Console y su licencia actual.

  El asistente simplifica la creación y configuración de una tarea de reparación de la vulnerabilidad y le permite eludir la creación de tareas redundantes que contienen las mismas actualizaciones para instalar.

Reparar vulnerabilidades de software a través de la lista de vulnerabilidades

Para reparar vulnerabilidades de software:

1. Abra una de las listas de vulnerabilidades:

   - Para abrir la lista general de vulnerabilidades, en el menú principal vaya a **Operaciones → Administración de parches → Vulnerabilidades de software**.

   - Para abrir la lista de vulnerabilidades de un dispositivo administrado, en el menú principal vaya a **Activos (dispositivos) → Dispositivos administrados → <nombre del dispositivo> → Avanzado → Vulnerabilidades de software**.

   - Para abrir la lista de vulnerabilidades de una aplicación específica, en el menú principal, vaya a **Operaciones → Aplicaciones de terceros → Registro de aplicaciones → <nombre de la aplicación> → Vulnerabilidades**.

   Se muestra una página con una lista de vulnerabilidades detectadas en las aplicaciones de terceros.

2. Seleccione una o más vulnerabilidades de la lista y haga clic en el botón **Reparar vulnerabilidad**.

   Si falta una actualización de software recomendada para reparar una de las vulnerabilidades seleccionadas, verá un mensaje informativo.

   Para reparar algunas vulnerabilidades de software, deberá aceptar un contrato de licencia de usuario final (EULA) que lo faculte a instalar el software. Si se le solicita aceptar el EULA, hágalo. Si rechaza el EULA, la vulnerabilidad de software correspondiente no se reparará.

3. Seleccione una de las siguientes opciones:

- **Nueva tarea**

  Se inicia el Asistente para crear nueva tarea. Dependiendo del modo de Kaspersky Security Center Cloud Console y su licencia actual, está preseleccionada la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Reparar vulnerabilidades*. Siga los pasos del asistente para completar la creación de la tarea.

- **Reparar vulnerabilidad (añadir regla a tarea específica)**

  Seleccione la tarea a la que desee agregar las vulnerabilidades seleccionadas. Dependiendo del modo de la Consola de Kaspersky Security Center Cloud Console y su licencia actual, seleccione una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o una tarea *Reparar vulnerabilidades*. Si selecciona una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, una nueva regla para corregir las vulnerabilidades seleccionadas se añadirá automáticamente a la tarea seleccionada. Si selecciona una tarea *Reparar vulnerabilidades*, las vulnerabilidades seleccionadas se añadirán a las propiedades de la tarea.

  Se abrirá la ventana de propiedades de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

Si optó por crear una tarea, se la creará y se la agregará a la lista de tareas disponible en **Activos (dispositivos)** → **Tareas**. Si optó por agregar las vulnerabilidades a una tarea existente, las vulnerabilidades se guardarán en las propiedades de la tarea que haya elegido.

Para reparar las vulnerabilidades de software de terceros, inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Reparar vulnerabilidades*. Si la tarea que creó es *Reparar vulnerabilidades*, deberá especificar manualmente qué actualizaciones se usarán para reparar las vulnerabilidades enumeradas en la configuración de la tarea.

Solucionar vulnerabilidades de software mediante el Asistente de reparación de vulnerabilidades

La disponibilidad del Asistente de reparación de vulnerabilidades depende de la licencia que utilice y del modo en el que Kaspersky Security Center Cloud Console esté funcionando.

Para corregir vulnerabilidades de software mediante el Asistente de reparación de vulnerabilidades:

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.

   Se muestra una página con una lista de las vulnerabilidades detectadas en las aplicaciones de terceros instaladas en los dispositivos administrados.

2. Active la casilla de verificación ubicada junto a la vulnerabilidad que desee reparar.

3. Haga clic en el botón **Ejecutar Asistente de reparación de vulnerabilidades**.

   Se inicia el Asistente de reparación de vulnerabilidades. En la página **Seleccionar tarea de reparación de la vulnerabilidad**, verá una lista con las tareas existentes de los siguientes tipos:

   - *Instalar actualizaciones requeridas y reparar vulnerabilidades*
   - *Instalar actualizaciones de Windows Update*
   - *Reparar vulnerabilidades*

   Los dos últimos tipos de tarea no se pueden modificar para instalar nuevas actualizaciones. Para instalar nuevas actualizaciones, solo puede utilizar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

4. Si desea que el asistente muestre solo las tareas que reparan la vulnerabilidad que ha seleccionado, active la opción **Mostrar solo las tareas que reparen esta vulnerabilidad**.

5. Elija lo que desea hacer:

   - Para iniciar una tarea, marque la casilla ubicada junto al nombre de la tarea en cuestión y haga clic en el botón **Iniciar**.

   - Para agregar una nueva regla a una tarea existente, haga lo siguiente:

     a. Marque la casilla ubicada junto al nombre de la tarea en cuestión y haga clic en el botón **Añadir regla**.

     b. En la página que se abre, configure la nueva regla:

     - Regla para reparar vulnerabilidades de este nivel de gravedad

       Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

       Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

       Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

       Esta opción está deshabilitada de manera predeterminada.

     - **Regla para reparar vulnerabilidades por medio de actualizaciones del mismo tipo que la actualización definida como recomendada para la vulnerabilidad seleccionada** (disponible solo para vulnerabilidades de software de Microsoft)

     - **Regla para reparar vulnerabilidades en aplicaciones del proveedor seleccionado** (disponible solo para vulnerabilidades de software de terceros)

     - **Regla para reparar una vulnerabilidad en todas las versiones de la aplicación seleccionada** (disponible solo para vulnerabilidades de software de terceros)

     - **Regla para reparar vulnerabilidad seleccionada**

     - Aprobar actualizaciones que reparen esta vulnerabilidad

       Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

       Esta opción está deshabilitada de manera predeterminada.

     c. Haga clic en el botón **Añadir**.

   - Para crear una tarea:

     a. Haga clic en el botón **Nueva tarea**.

     b. En la página que se abre, configure la nueva regla:

- Regla para reparar vulnerabilidades de este nivel de gravedad

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

  Esta opción está deshabilitada de manera predeterminada.

- **Regla para reparar vulnerabilidades mediante actualizaciones del tipo** (disponible solo para vulnerabilidades de software de Microsoft)
- **Regla para reparar vulnerabilidades en aplicaciones del proveedor seleccionado** (disponible solo para vulnerabilidades de software de terceros)
- **Regla para reparar una vulnerabilidad en todas las versiones de la aplicación seleccionada** (disponible solo para vulnerabilidades de software de terceros)
- **Regla para reparar vulnerabilidad seleccionada**
- Aprobar actualizaciones que reparen esta vulnerabilidad

  Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

  Esta opción está deshabilitada de manera predeterminada.

c. Haga clic en el botón **Añadir**.

Si ha elegido iniciar una tarea, puede cerrar el asistente. La tarea se completará en segundo plano. No se requieren más acciones.

Si optó por agregar una regla a una tarea existente, se abrirá la ventana de propiedades de la tarea. Encontrará la nueva regla en las propiedades de la tarea. Si lo desea, vea y modifique la regla u otros ajustes de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

Si eligió crear una tarea, siga creando la tarea en el Asistente para crear nueva tarea. La nueva regla que añadió en el Asistente de reparación de vulnerabilidades se muestra en el Asistente para crear nueva tarea. Cuando completa el Asistente para crear nueva tarea, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se añade a la lista de tareas.

Crear la tarea Reparar vulnerabilidades

La tarea *Reparar vulnerabilidades* le permite corregir vulnerabilidades en el software de Microsoft instalado en dispositivos administrados que ejecutan Windows.

La disponibilidad de esta función depende del modo de Kaspersky Security Center Cloud Console y su licencia actual. Le recomendamos que utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* en lugar de la tarea *Reparar vulnerabilidades*. La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* le permitirá instalar varias actualizaciones y reparar varias vulnerabilidades automáticamente utilizando un conjunto de reglas.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia de uso de Kaspersky Security Center Cloud Console y el modo de funcionamiento de Kaspersky Security Center Cloud Console.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedírsele al usuario que la cierre.

Para crear la tarea Reparar vulnerabilidades:

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 Cloud Console, seleccione el tipo de tarea **Reparar vulnerabilidades**.
4. Escriba un nombre para la tarea que está creando.

   El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Seleccione los dispositivos a los que se asignará la tarea.
6. Haga clic en el botón **Añadir**.

   Se abre la lista de vulnerabilidades.
7. Seleccione las vulnerabilidades que desee reparar y, a continuación, haga clic en **Aceptar**.
8. Defina las opciones de reinicio del sistema operativo:

   - **No reiniciar el dispositivo**

     Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o 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)**

  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.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está 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.

9. Configure los ajustes relativos a la cuenta:

- **Cuenta predeterminada**

  La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

  Esta opción está seleccionada de 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.

10. 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.

11. Haga clic en el botón **Finalizar**.

    Se crea la tarea y se la agrega a la lista de tareas.

12. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

13. En la ventana de propiedades de la tarea, modifique los ajustes generales de la tarea según resulte necesario.

14. Haga clic en el botón **Guardar**.

La tarea queda creada y configurada.

Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades

La disponibilidad de la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* depende del modo de consola de Kaspersky Security Center Cloud Console y de su licencia actual.

Utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para aplicar actualizaciones y reparar vulnerabilidades en las aplicaciones de terceros (incluidas las de Microsoft) instaladas en los dispositivos administrados. Esta tarea le permite instalar múltiples actualizaciones y corregir múltiples vulnerabilidades de acuerdo con ciertas reglas.

Si desea usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar actualizaciones o reparar vulnerabilidades, realice alguna de las siguientes acciones:

- Ejecute el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.
- Cree una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Agregue una regla de instalación de actualizaciones a una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* existente.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia de uso de Kaspersky Security Center Cloud Console y el modo de funcionamiento de Kaspersky Security Center Cloud Console.

Para crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades:

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 Cloud Console, seleccione el tipo de tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Seleccione los dispositivos a los que se asignará la tarea.
6. Defina las reglas de instalación de actualizaciones y luego configure los siguientes ajustes:

   - **Iniciar la instalación al reiniciar o apagar el dispositivo**

     Si esta opción está habilitada, las actualizaciones se instalarán en el momento en el que los dispositivos se reinicien o se apaguen. De lo contrario, las actualizaciones se instalarán siguiendo la programación que se defina.

     Utilice esta opción si la instalación de las actualizaciones podría afectar el rendimiento de los dispositivos.

     Esta opción está deshabilitada de manera predeterminada.

   - **Instalar los componentes generales del sistema necesarios**

     Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Por ejemplo, estos requisitos previos pueden ser actualizaciones del sistema operativo.

     Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

     Esta opción está deshabilitada de manera predeterminada.

   - **Autorizar la instalación de las nuevas versiones de la aplicación durante las actualizaciones**

     Si esta opción está habilitada, las actualizaciones podrán cambiar la versión del software actualizado por una más reciente.

     Si esta opción está deshabilitada, los cambios de versión no estarán permitidos. Para instalar una versión más reciente de una aplicación, deberá usar una tarea diferente o proceder en forma manual. Podría usar esta opción si, por ejemplo, desea evaluar el cambio de versión en una infraestructura de prueba o si sabe que la versión más reciente no es compatible con la infraestructura de su empresa.

     Esta opción está habilitada de manera predeterminada.

     Los cambios de versión pueden ocasionar problemas de funcionamiento en las aplicaciones dependientes instaladas en los dispositivos cliente.

   - **Descargar actualizaciones en el dispositivo sin instalarlas**

Si esta opción está habilitada, la aplicación descargará las actualizaciones disponibles en los dispositivos, pero no las instalará automáticamente. Podrá instalar las actualizaciones descargadas manualmente.

Las actualizaciones de Microsoft se descargan en el sistema de almacenamiento de Windows. Las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft) se descargan en la carpeta especificada en el campo **Descargar actualizaciones en**.

Si esta opción está deshabilitada, las actualizaciones se instalarán en los dispositivos automáticamente.

Esta opción está deshabilitada de manera predeterminada.

- **Descargar actualizaciones en**

  Esta carpeta se utiliza para descargar las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft).

- **Activar diagnóstico avanzado**

  Si esta función está activada, el Agente de red escribe los rastreos incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center Cloud Console. Los datos de seguimiento se guardan en dos archivos sucesivamente; el tamaño total de ambos archivos está determinado por el valor de la opción **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando los archivos alcanzan su límite de tamaño, el Agente de red comienza a sobrescribirlos. Los archivos de seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está desactivada, el Agente de red escribe rastros de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center Cloud Console. No se guardará ningún otro dato de seguimiento.

  No es necesario que habilite la característica de diagnóstico avanzado al momento de crear una tarea. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está deshabilitada de manera predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

7. Especifique la configuración 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)**

  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.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está habilitada de manera predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Tiempo de espera antes del cierre forzado de aplicaciones en sesiones bloqueadas (min)**

  Las aplicaciones se cerrarán por la fuerza cuando el dispositivo del usuario se bloquee (sea manualmente o en forma automática tras un tiempo de inactividad).

  Si esta opción está habilitada, las aplicaciones del dispositivo bloqueado se cerrarán por la fuerza luego de transcurra el intervalo especificado en el campo de entrada.

  Si esta opción está deshabilitada, las aplicaciones del dispositivo bloqueado no se cerrarán.

  Esta opción está deshabilitada de manera predeterminada.

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.

Si el resultado de la tarea contiene una advertencia sobre el error 0x80240033, deberá recurrir al Registro de Windows para resolver el inconveniente. El error indica lo siguiente: "Error del Agente de Windows Update 80240033 ("No se pudieron descargar los términos de licencia.")".

Agregar reglas de instalación de actualizaciones

La disponibilidad de esta función depende del modo de Kaspersky Security Center Cloud Console y su licencia actual.

Si desea utilizar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar actualizaciones de software o reparar vulnerabilidades en sus aplicaciones, debe definir reglas de instalación de actualizaciones. Estas reglas determinan qué actualizaciones se deben instalar y qué vulnerabilidades se deben reparar.

La configuración exacta depende de si la regla se crea para todas las actualizaciones, para actualizaciones de Windows Update o para actualizaciones publicadas para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky y Microsoft). Cuando agregue una regla para actualizaciones de Windows Update o para actualizaciones de aplicaciones de terceros, podrá seleccionar las aplicaciones específicas (y las versiones puntuales de esas aplicaciones) para las que quiera instalar actualizaciones. Cuando agregue una regla para todas las actualizaciones, podrá seleccionar las actualizaciones específicas que quiera instalar y las vulnerabilidades puntuales que quiera reparar mediante la instalación de actualizaciones.

Para agregar una regla de instalación de actualizaciones, puede optar por cualquiera de estos métodos:

- Al añadir una regla mientras crea una nueva tarea Instalar actualizaciones requeridas y reparar vulnerabilidades.
- Agregue la regla en la pestaña **Configuración de la aplicación** de la ventana de propiedades de una tarea de *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Mediante el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.

Para agregar una nueva regla para todas las actualizaciones:

1. Haga clic en el botón **Añadir**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Next**.

2. En la página **Tipo de regla**, seleccione **Regla para todas las actualizaciones**.

3. En la página **Criterios generales**, use las listas desplegables para definir los siguientes ajustes:

   - **Conjunto de actualizaciones para instalar**

Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

- **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
- **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
- **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

- Reparar vulnerabilidades con un nivel de gravedad igual o mayor que

Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

Esta opción está deshabilitada de manera predeterminada.

4. En la página **Actualizaciones**, seleccione las actualizaciones que se instalarán:

- Instalar todas las actualizaciones pertinentes

Instalar todas las actualizaciones de software que cumplan con los criterios especificados en la página de **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

- Instalar solo las actualizaciones de la lista

Se instalarán únicamente las actualizaciones de software que seleccione manualmente en la lista. La lista contiene todas las actualizaciones de software disponibles.

Existen situaciones en las que querrá elegir manualmente las actualizaciones que se instalarán: podría suceder, por ejemplo, que quiera evaluar ciertas actualizaciones en un entorno de prueba, que quiera actualizar solo las aplicaciones que considere importantes o que necesite actualizar solo algunas aplicaciones puntuales.

- Instalar automáticamente todas las actualizaciones anteriores de la aplicación que se requieren para instalar las actualizaciones seleccionadas

Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

Esta opción está habilitada de manera predeterminada.

5. En la página **Vulnerabilidades**, seleccione las vulnerabilidades que se repararán al instalar las actualizaciones seleccionadas:

   - **Reparar todas las vulnerabilidades que coinciden con otros criterios**

     Reparar todas las vulnerabilidades que cumplan con los criterios especificados en la página de **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

   - **Reparar solo las vulnerabilidades de la lista**

     Se repararán únicamente las vulnerabilidades que seleccione manualmente en la lista. La lista contiene todas las vulnerabilidades detectadas.

     Existen situaciones en las que querrá elegir manualmente las vulnerabilidades que se repararán: podría suceder, por ejemplo, que quiera verificar en un entorno de prueba que las vulnerabilidades se puedan reparar, que quiera reparar las vulnerabilidades solo en las aplicaciones que considere importantes o que prefiera reparar las vulnerabilidades solo en ciertas aplicaciones puntuales.

6. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Una vez que el Asistente de creación de reglas finaliza su operación, la nueva regla se añade y se muestra en el campo del Asistente para crear nueva tarea.

Para agregar una nueva regla para actualizaciones de Windows Update:

1. Haga clic en el botón **Añadir**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Next**.

2. En la página **Tipo de regla**, seleccione **Regla para Windows Update**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

   - **Conjunto de actualizaciones para instalar**

Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

- **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
- **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
- **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

- Reparar vulnerabilidades con un nivel de gravedad igual o mayor que

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

  Esta opción está deshabilitada de manera predeterminada.

- Reparar vulnerabilidades con un nivel de gravedad MSRC igual o mayor que

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

  Esta opción está deshabilitada de manera predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Categorías de actualizaciones**, seleccione las categorías de actualizaciones que se instalarán. Las categorías son las mismas que se usan en el Catálogo de Microsoft Update. Por defecto, están seleccionadas todas las categorías.

6. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Una vez que el Asistente de creación de reglas finaliza su operación, la nueva regla se añade y se muestra en el campo del Asistente para crear nueva tarea.

Para agregar una nueva regla para actualizaciones de aplicaciones de terceros:

1. Haga clic en el botón **Añadir**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Next**.

2. En la página **Tipo de regla**, seleccione **Regla para actualizaciones de terceros**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - Reparar vulnerabilidades con un nivel de gravedad igual o mayor que

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar el nivel de gravedad.

     Esta opción está deshabilitada de manera predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección Configuración de la ventana de propiedades de la tarea creada.

Una vez que el Asistente de creación de reglas finaliza su operación, la nueva regla se añade y se muestra en el campo del Asistente para crear nueva tarea.

Ver información sobre las vulnerabilidades de software detectadas en todos los dispositivos administrados

Si ya ha analizado el software de los dispositivos administrados en busca de vulnerabilidades, puede ver la lista de vulnerabilidades de software detectadas en la totalidad de los dispositivos administrados. Si ejecuta la tarea para la jerarquía de Servidores de administración, puede ver la lista de dispositivos administrados con vulnerabilidades detectadas solo para el Servidor de administración seleccionado.

Para ver la lista de vulnerabilidades de software detectadas en todos los dispositivos administrados:

En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.

La página muestra la lista de vulnerabilidades de software detectadas en los dispositivos cliente.

También puede generar y ver un Informe de vulnerabilidades.

Puede aplicar un filtro para ver la lista de vulnerabilidades de software. Para definir el filtro, haga clic en el ícono **Filtro** ( ) ubicado en la esquina superior derecha de la lista de vulnerabilidades de software. También puede elegir un filtro preestablecido de la lista desplegable **Preestablecer filtros**, que se encuentra sobre la lista de vulnerabilidades de software.

Puede obtener información detallada sobre cualquiera de las vulnerabilidades de la lista.

Para obtener información sobre una vulnerabilidad de software:

En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de su interés.

Se abre la ventana de propiedades de la vulnerabilidad de software.

Ver información sobre las vulnerabilidades de software detectadas en un dispositivo administrado específico

Puede ver información sobre las vulnerabilidades de software detectadas en un dispositivo administrado específico que ejecute Windows.

Para ver la lista de las vulnerabilidades de software detectadas en el dispositivo administrado seleccionado:

1. En el menú principal, vaya a **Activos (dispositivos)**→ **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo para el que desee ver las vulnerabilidades de software detectadas.

   Se muestra la ventana de propiedades del dispositivo seleccionado.

3. En la ventana de propiedades del dispositivo seleccionado, elija la pestaña **Avanzado**.

4. En el panel izquierdo, seleccione la sección **Vulnerabilidades de software**.

Se muestra la lista de vulnerabilidades de software detectadas en el dispositivo administrado que seleccionó.

Para ver las propiedades de una vulnerabilidad de software específica:

En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de software que sea de su interés.

Se muestra la ventana de propiedades de la vulnerabilidad de software seleccionada.

Ver estadísticas de las vulnerabilidades presentes en los dispositivos administrados

Puede ver estadísticas sobre cada vulnerabilidad de software detectada en los dispositivos administrados. Las estadísticas se presentan en forma de diagrama. El diagrama muestra la cantidad de dispositivos con los siguientes estados:

- *Ignorada en: <cantidad de dispositivos>*. Este estado se asigna cuando la vulnerabilidad se desestima manualmente a través de sus propiedades.
- *Reparada en: <cantidad de dispositivos>*. Este estado se asigna cuando la tarea para reparar la vulnerabilidad se completa correctamente.
- *Reparación programada para: <cantidad de dispositivos>*. Este estado se asigna cuando se ha creado una tarea para reparar la vulnerabilidad, pero aún no se la ha ejecutado.
- *Parche aplicado en: <cantidad de dispositivos>*. Este estado se asigna cuando se ha elegido manualmente una actualización de software que debía reparar la vulnerabilidad, pero no la ha reparado.
- *Debe repararse en: <cantidad de dispositivos>*. Este estado se asigna si la vulnerabilidad se corrigió solo en algunos dispositivos administrados y es necesario corregirla en más dispositivos administrados.

Para ver las estadísticas de una vulnerabilidad en los dispositivos administrados:

1. En el menú principal, vaya a **Operaciones → Administración de parches → Vulnerabilidades de software**.

   La página muestra una lista con las vulnerabilidades detectadas en las aplicaciones de los dispositivos administrados.

2. Active la casilla de verificación ubicada junto a la vulnerabilidad de su interés.

3. Haga clic en el botón **Estadísticas de vulnerabilidades en dispositivos**.

   Se muestra un diagrama con los estados de la vulnerabilidad. Para ver los dispositivos en los que la vulnerabilidad tenga un estado en particular, haga clic en ese estado.

Exportar la lista de vulnerabilidades de software a un archivo

Puede exportar la lista de vulnerabilidades que se muestra en la aplicación a un archivo CSV o TXT. Una vez que tenga el archivo, podrá almacenarlo para fines estadísticos, enviarlo a la persona que esté a cargo de la seguridad de la información o utilizarlo para otros fines.

Para exportar a un archivo de texto la lista de vulnerabilidades de software detectadas en todos los dispositivos administrados:

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.

   La página muestra una lista con las vulnerabilidades detectadas en las aplicaciones de los dispositivos administrados.

2. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera.

El archivo con la lista de vulnerabilidades de software se guardará en el dispositivo que esté utilizando.

Para exportar a un archivo de texto la lista de vulnerabilidades de software detectadas en un dispositivo administrado específico:

1. Abra la lista de vulnerabilidades de software detectadas en el dispositivo administrado de su interés.

2. Seleccione las vulnerabilidades de software que desee exportar.

   Omita este paso si desea exportar toda la lista de vulnerabilidades de software detectadas en el dispositivo administrado.

   Si desea exportar la lista completa de vulnerabilidades de software detectadas en el dispositivo administrado, tenga en cuenta que solo se exportarán las vulnerabilidades enumeradas en la página que esté viendo.

3. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera.

En el dispositivo que esté utilizando, se guardará un archivo con la lista de vulnerabilidades de software detectadas en el dispositivo administrado que haya seleccionado.

Ignorar vulnerabilidades de software

Puede ignorar las vulnerabilidades de software que no desee reparar. Hay distintos motivos para ignorar una vulnerabilidad de software, por ejemplo:

- no considera que la vulnerabilidad de software sea de extrema importancia para su organización;
- entiende que, al reparar la vulnerabilidad, se pondrían en riesgo los datos vinculados al software vulnerable;
- sabe que la vulnerabilidad de software no es un riesgo para la red de su organización porque utiliza otras medidas para proteger sus dispositivos administrados.

Puede ignorar una vulnerabilidad de software en todos los dispositivos administrados o solo en los dispositivos administrados que usted seleccione.

Para ignorar una vulnerabilidad de software en todos los dispositivos administrados:

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.

   La página muestra una lista con las vulnerabilidades de software detectadas en los dispositivos administrados.

2. En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de software que desee ignorar.

   Se abre la ventana de propiedades de la vulnerabilidad de software.

3. En la pestaña **General**, habilite la opción **Ignorar vulnerabilidad**.

4. Haga clic en el botón **Guardar**.

   Se cierra la ventana de propiedades de la vulnerabilidad de software.

La vulnerabilidad de software se ignorará en todos los dispositivos administrados.

Para ignorar una vulnerabilidad de software en un dispositivo administrado específico:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo en el que desee ignorar la vulnerabilidad de software.

   Se abre la ventana de propiedades del dispositivo.

3. En la ventana de propiedades del dispositivo, seleccione la pestaña **Avanzado**.

4. En el panel izquierdo, seleccione la sección **Vulnerabilidades de software**.

   Se muestra la lista de vulnerabilidades de software detectadas en el dispositivo.

5. En la lista de vulnerabilidades de software, seleccione la vulnerabilidad que desee ignorar en el dispositivo seleccionado.

   Se abre la ventana de propiedades de la vulnerabilidad de software.

6. En la ventana de propiedades de la vulnerabilidad de software, en la pestaña **General**, habilite la opción **Ignorar vulnerabilidad**.

7. Haga clic en el botón **Guardar**.

   Se cierra la ventana de propiedades de la vulnerabilidad de software.

8. Cierre la ventana de propiedades del dispositivo.

La vulnerabilidad de software se ignorará en el dispositivo seleccionado.

Cuando se completen las tareas *Reparar vulnerabilidades* o *Instalar actualizaciones requeridas y reparar vulnerabilidades*, la vulnerabilidad de software ignorada no se reparará. Las vulnerabilidades de software desestimadas pueden excluirse de la lista de vulnerabilidades a través del filtro.

Escenario: encontrar y corregir vulnerabilidades de software

En esta sección, se describe un escenario para buscar y reparar vulnerabilidades en dispositivos administrados que utilizan el sistema operativo Windows. Puede encontrar y corregir vulnerabilidades de software en el sistema operativo y en el software de terceros, incluido el software de Microsoft.

Requisitos previos

- Kaspersky Security Center Cloud Console está implementada en su organización.
- Hay dispositivos administrados que ejecutan Windows en su organización.

Etapas

El proceso para buscar y reparar vulnerabilidades de software se divide en etapas:

1. **Escaneo de vulnerabilidades en el software instalado en los dispositivos cliente**

   Para encontrar vulnerabilidades en el software instalado en los dispositivos administrados, ejecute la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, Kaspersky Security Center Cloud Console recibe las listas de vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos que especificó en las propiedades de la tarea.

   La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente con el asistente de inicio rápido de Kaspersky Security Center Cloud Console. Si no ejecutó el asistente, hágalo ahora o cree la tarea manualmente.

   Instrucciones prácticas: Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas

2. **Analizar la lista de vulnerabilidades de software detectadas**

   Abra la lista **Vulnerabilidades de software** y decida qué vulnerabilidades desea reparar. Para ver información detallada sobre una vulnerabilidad, haga clic en el nombre de la misma en la lista. La aplicación le da acceso a estadísticas sobre el estado de cada vulnerabilidad en los dispositivos administrados.

   Instrucciones:

   - Consulta de información sobre las vulnerabilidades de software
   - Ver estadísticas de las vulnerabilidades presentes en los dispositivos administrados

3. **Configurar la reparación de vulnerabilidades**

   Una vez que se han detectado las vulnerabilidades de software, puede repararlas en los dispositivos administrados con las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades* y *Reparar vulnerabilidades*.

   Utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para aplicar actualizaciones y reparar vulnerabilidades en las aplicaciones de terceros (incluidas las de Microsoft) instaladas en los dispositivos administrados. Esta tarea le permite instalar múltiples actualizaciones y corregir múltiples vulnerabilidades de acuerdo con ciertas reglas. La disponibilidad de esta tarea depende del modo de Kaspersky Security Center Cloud Console y de su licencia actual. Para corregir vulnerabilidades de software, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* utiliza las actualizaciones de software recomendadas.

   La tarea *Reparar vulnerabilidades* utiliza las correcciones recomendadas para el software de Microsoft.

   Puede iniciar el Asistente de reparación de vulnerabilidades que crea una de estas tareas automáticamente, o puede crear una de estas de forma manual.

   Instrucciones: Reparación de vulnerabilidades en software de terceros, Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades

4. **Programar las tareas**

   Para asegurarse de que la lista de vulnerabilidades siempre esté actualizada, defina una programación que haga que la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecute automáticamente de tanto en tanto. Se recomienda una frecuencia promedio de una vez a la semana.

   Si ha creado la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede programarla para que se ejecute con igual o menor frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Al programar la tarea *Reparar vulnerabilidades*, tenga en cuenta que debe seleccionar soluciones para el software de Microsoft cada vez antes de comenzar la tarea.

   Cuando programe las tareas, asegúrese de que las tareas para reparar vulnerabilidades se inicien después de que finalice la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

5. **Ignorar vulnerabilidades de software (opcional)**

Puede ignorar aquellas vulnerabilidades de software que no desee reparar en ninguno de los dispositivos administrados o en algunos dispositivos administrados específicos.

Instrucciones: Ignorar las vulnerabilidades del software

6. **Ejecutar una tarea de reparación de vulnerabilidades**

   Inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Reparar vulnerabilidades*. Cuando se complete la tarea ejecutada, verifique que su estado en la lista de tareas sea *Completada correctamente*.

7. **Crear el informe sobre los resultados de la reparación de vulnerabilidades de software (opcional)**

   Para ver estadísticas detalladas sobre la reparación de vulnerabilidades, genere el Informe de vulnerabilidades. El informe le indicará qué vulnerabilidades de software no se corrigieron. Ello le dará un panorama sobre la búsqueda y reparación de vulnerabilidades en el software de terceros (incluido el software de Microsoft) instalado en su organización.

   Instrucciones: Generar y ver un informe

8. **Revisar la configuración de la búsqueda y reparación de vulnerabilidades en el software de terceros**

   Asegúrese de lo siguiente:

   - La lista de vulnerabilidades de software en dispositivos administrados no esté vacía.
   - Una tarea para corregir vulnerabilidades está en la lista de tareas.
   - Las tareas para buscar y reparar vulnerabilidades de software se programan de manera tal que comiencen secuencialmente. Vea las propiedades de estas tareas y compare su programación.
   - La tarea para reparar vulnerabilidades de software se ha completado correctamente. Vea la información en la pestaña **Resultados** en la ventana de las propiedades de la tarea.

Resultados

Si creó y configuró la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las vulnerabilidades se repararán en los dispositivos administrados automáticamente. Cuando se ejecuta, la tarea compara la lista de actualizaciones de software disponibles con las reglas especificadas en su configuración. Todas las actualizaciones de software que cumplan con los criterios especificados en las reglas se descargarán en los repositorios de los puntos de distribución y se instalarán para reparar las vulnerabilidades de software, salvo Windows Update. Para instalar Windows Update, debe garantizar el acceso a los servidores públicos de Windows Update en sus dispositivos administrados.

Si creó la tarea *Reparar vulnerabilidades*, solo se corregirán las vulnerabilidades presentes en el software de Microsoft.

Configurar el período máximo de almacenamiento para la información sobre las vulnerabilidades reparadas

Para definir el tiempo por el que la base de datos conservará información sobre las vulnerabilidades reparadas en los dispositivos administrados:

1. 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 página que se abre, vaya a la pestaña **Repositorio de eventos** tab.

3. Especifique el periodo máximo de almacenamiento de la información sobre las vulnerabilidades reparadas en la base de datos.

   De manera predeterminada, el periodo de almacenamiento es de 7 días en el modo de prueba y de 60 días en el modo comercial. El límite máximo es de 14 días en el modo de prueba y de 365 días en el modo comercial.

4. Haga clic en **Guardar**.

El período de almacenamiento para la información sobre las vulnerabilidades reparadas queda limitado al número de días especificado.

Administración de las aplicaciones que se ejecutan en los dispositivos cliente

Esta sección describe las funciones de Kaspersky Security Center Cloud Console relacionadas con la administración de aplicaciones ejecutadas en dispositivos cliente.

Uso de Control de aplicaciones para administrar archivos ejecutables

Puede utilizar el componente Control de aplicaciones para permitir o bloquear el inicio de archivos ejecutables en dispositivos de usuario. El componente Control de aplicaciones es compatible con sistemas operativos basados en Windows y 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 Cloud Console está implementada en su organización.
- Se ha creado y activado una directiva para Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security para Windows.

Etapas

El escenario de uso de Control de aplicaciones procede en etapas:

1. **Crear y ver la lista de archivos ejecutables almacenados en los dispositivos cliente**

   En esta etapa, podrá descubrir qué archivos ejecutables se encuentran guardados en los dispositivos administrados. Revise la lista de archivos ejecutables y compárela con las listas de archivos ejecutables permitidos y prohibidos. Las restricciones sobre el uso de archivos ejecutables pueden estar vinculadas a las políticas de seguridad de la información de su organización.

   Instrucciones: Obtener y ver una lista de archivos ejecutables instalada en dispositivos cliente

2. **Crear categorías para los archivos ejecutables que se usan en su organización**

Analizar las listas de archivos ejecutables almacenados en los dispositivos administrados. Cree categorías para archivos ejecutables sobre la base del análisis. Recomendamos crear una categoría llamada "Aplicaciones de trabajo" que cubra el conjunto estándar de archivos ejecutables que se utilizan en la organización. A continuación, si tiene distintos grupos de seguridad que trabajan con diferentes archivos ejecutables, puede crear una categoría por separado para cada grupo de seguridad.

Instrucciones: Crear categoría de aplicación con contenido agregado manualmente, Crear una categoría de aplicación que incluya archivos ejecutables de dispositivos seleccionados

3. **Configurar Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows**

   Configure el componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security for Windows con las categorías que ha creado en la etapa anterior.

   Instrucciones: Configuración de Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows.

4. **Activar el componente Control de aplicaciones en modo de prueba**

   Las reglas de Control de aplicaciones no deben bloquear los archivos ejecutables que los usuarios necesitan para trabajar. Para asegurarse de que esto sea así, cuando cree nuevas reglas de Control de aplicaciones, recomendamos que active una prueba de las reglas y analice su funcionamiento. Mientras estas pruebas se encuentren activas, Kaspersky Endpoint Security para Windows no bloqueará los archivos ejecutables que las reglas de Control de aplicaciones no permitan iniciar, sino que simplemente notificará al Servidor de administración para informar de que tales aplicaciones se han 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: Configuración del componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y active el modo de prueba en el proceso de configuración.

5. **Cambiar la configuración de las categorías en el componente Control de aplicaciones**

   De ser necesario, modifique la configuración de Control de aplicaciones. Con los resultados de las pruebas, puede crear una categoría de aplicaciones con contenido agregado manualmente que incluya los archivos ejecutables vinculados a los eventos de Control de aplicaciones.

   Instrucciones: Añadir archivos ejecutables relacionados con eventos a la categoría de la aplicación

6. **Aplicar las reglas de Control de aplicaciones en modo de funcionamiento normal**

   Después de probar las reglas de Control de aplicaciones y completar la configuración de las categorías, podrá aplicar las reglas de Control de aplicaciones en el modo de operación.

   Instrucciones: Configuración del componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y desactive el modo de prueba en el proceso de configuración.

7. **Verificar la configuración de Control de aplicaciones**

   Asegúrese de lo siguiente:

   - La lista de categorías de archivos ejecutables no está vacía. Vea la lista de categorías de aplicaciones y asegúrese de que contenga las categorías que ha configurado.
   - El control de aplicaciones se configura utilizando categorías creadas para archivos ejecutables. Vea la configuración de la directiva de Kaspersky Endpoint Security para Windows y asegúrese de haber configurado el Control de aplicaciones en **Configuración de aplicaciones** → **Controles de seguridad** → **Control de aplicaciones**.

- Las reglas del Control de aplicaciones se aplican en el modo de operación. Verifique el modo en la directiva de Kaspersky Endpoint Security para Windows y asegúrese de haber desactivado el **Modo de prueba** en **Configuración de aplicaciones → Controles de seguridad → Control de aplicaciones**.

Resultados

Al concluir este escenario, la ejecución de archivos ejecutables en los dispositivos administrados estará bajo su control. Los usuarios pueden iniciar solo aquellos archivos ejecutables que están permitidos en su organización, no los que están prohibidos.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux

Modos y categorías de Control de aplicaciones

El componente Control de aplicaciones supervisa los intentos de los usuarios de iniciar archivos ejecutables. Puede usar las reglas de Control de aplicaciones para vigilar el inicio de archivos ejecutables.

El componente Control de aplicaciones está disponible para Kaspersky Endpoint Security para Windows y para Kaspersky Endpoint Security for Linux (versión 11.2 y posteriores). Todas las instrucciones de esta sección describen la configuración del Control de aplicaciones para Kaspersky Endpoint Security.

Cuando un archivo ejecutable no está alcanzado por una regla de Control de aplicaciones, la posibilidad de que se permita ejecutarlo depende del modo de funcionamiento del componente:

- *Lista de rechazados*. En este modo, se permite la ejecución de cualquier archivo ejecutable, excepto los especificados en reglas de bloqueo. El modo *Lista de rechazados* está seleccionado de forma predeterminada.
- *Lista de admitidos*. En este modo, se impide la ejecución de todos los archivos ejecutables, excepto los especificados en reglas de autorización.

Las reglas de Control de aplicaciones se implementan a través de categorías para archivos ejecutables. En Kaspersky Security Center Cloud Console hay dos tipos de categorías de aplicaciones:

- Categorías con contenido agregado de forma manual. Para sumar archivos ejecutables a una categoría de este tipo, deberá definir distintas condiciones: metadatos del archivo, código hash del archivo, certificado del archivo, categoría KL, ruta de acceso al archivo, etc.
- Categoría que incluye los archivos ejecutables de los dispositivos seleccionados. Para crear una categoría de este tipo, deberá seleccionar un dispositivo. Los archivos ejecutables de ese dispositivo se agregarán a la categoría automáticamente.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux

Obtener y ver una lista de aplicaciones instaladas en los dispositivos cliente

Kaspersky Security Center Cloud Console 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, el nombre del proveedor, número de versión, lista de archivos ejecutables, lista de dispositivos en los que está instalada la aplicación, lista de actualizaciones de software disponibles o la lista de vulnerabilidades de software detectadas.

2. Puede agrupar y filtrar los datos de la tabla con las aplicaciones instaladas de la siguiente manera:

   - Haga clic en el icono de configuración ( ) en la esquina superior derecha de la tabla.

     En el menú invocado **Configuración de las columnas**, seleccione las columnas que se mostrarán en la tabla. Para ver el tipo de sistema operativo de los dispositivos cliente en los que está instalada la aplicación, seleccione la columna **Tipo de sistema operativo**.

   - Haga clic en el icono de filtro ( ) en la esquina superior derecha de la tabla y luego especifique y aplique el criterio de filtro en el menú invocado.

     Se muestra la tabla filtrada de aplicaciones instaladas.

Para visualizar la lista de aplicaciones instaladas en un dispositivo administrado en particular:

En el menú principal, vaya a **Dispositivos** → **Dispositivos administrados** → **<device name>** → **Avanzado** → **Registro de aplicaciones**. En este menú, puede exportar la lista de aplicaciones a un archivo CSV o TXT.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux

Obtener y ver una lista de archivos ejecutables instalada en dispositivos cliente

Puede obtener la lista de archivos ejecutables almacenados en los dispositivos cliente de una de las siguientes maneras:

- Habilitando las notificaciones sobre el inicio de aplicaciones en la directiva de Kaspersky Endpoint Security.

- Creando una tarea de inventario.

Habilitando las notificaciones sobre el inicio de aplicaciones en la directiva de Kaspersky Endpoint Security

Para habilitar las notificaciones sobre la ejecución de aplicaciones:

1. Abra la configuración de la directiva de Kaspersky Endpoint Security y luego vaya a **Configuración general** → **Informes y almacenamiento**.
2. En el grupo de configuración **Transferencia de datos al servidor de administración**, seleccione la casilla de verificación **Acerca de las aplicaciones iniciadas** y guarde los cambios.

Cuando un usuario intenta iniciar archivos ejecutables, la información sobre estos archivos se añade a la lista de archivos ejecutables en el dispositivo cliente. Kaspersky Endpoint Security envía esta información al Agente de red, que a su vez la envía al Servidor de administración.

Crear una tarea de inventario

La función de inventario de archivos ejecutables está disponible para las siguientes aplicaciones:

- Kaspersky Endpoint Security para Windows
- Kaspersky Endpoint Security for Linux (versión 11.2 y posteriores)

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 preferible de dispositivos es de 1 a 3.

Desaconsejamos ejecutar la tarea de inventario si se utilizan las siguientes bases de datos: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (todas las ediciones).

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 **Configuración de tarea nueva**, en la lista desplegable **Aplicación**, elija Kaspersky Endpoint Security para Windows o Kaspersky Endpoint Security for Linux, según el tipo de sistema operativo de los dispositivos cliente.
4. En la lista desplegable **Tipo de tarea**, seleccione **Inventario**.
5. En la página **Finalizar la creación de tareas**, haga clic en el botón **Finalizar**.

Una vez que se completa el Asistente para crear nueva tarea, se crea y configura la tarea **Inventario**. Si lo desea, puede cambiar la configuración de la tarea creada. Encontrará la nueva tarea en la lista de tareas.

Para obtener una descripción detallada de la tarea de inventario, consulte las siguientes ayudas:

- Ayuda de Kaspersky Endpoint Security para Windows
- Ayuda de Kaspersky Endpoint Security for Linux

Después de realizar la tarea **Inventario**, se forma la lista de archivos ejecutables instalados en los dispositivos administrados y puede ver la lista.

Durante el inventario, se pueden detectar los siguientes formatos de archivos ejecutables (dependiendo de la opción que seleccione en las propiedades de la tarea de inventario): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR y HTML.

Consultar las listas de archivos ejecutables almacenados en los dispositivos administrados

Haga lo siguiente para ver una lista de los archivos ejecutables almacenados en dispositivos cliente:

En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Archivos ejecutables**.

La página muestra la lista de los archivos ejecutables instalados en dispositivos cliente.

Si es necesario, puede enviar el archivo ejecutable del dispositivo administrado al dispositivo donde está abierto su Kaspersky Security Center Cloud Console.

Para enviar un archivo ejecutable:

1. En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Archivos ejecutables**.
2. Haga clic en el enlace del archivo ejecutable que desea enviar.
3. En la ventana que se abre, vaya a la sección **Dispositivos** y seleccione la casilla del dispositivo administrado desde el que desea enviar el archivo ejecutable.

   Antes de enviar el archivo ejecutable, marque la casilla **No desconectar del Servidor de administración** para asegurarse de que el dispositivo administrado tenga una conexión directa con el Servidor de administración. El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

4. Haga clic en el botón **Enviar**.

El archivo ejecutable seleccionado se descarga para su posterior envío al dispositivo donde está abierta su Kaspersky Security Center Cloud Console.

Crear una categoría de aplicaciones con contenido agregado manualmente

Puede especificar un conjunto de criterios que sean comunes a los archivos ejecutables que los usuarios podrán o no podrán iniciar en su organización. Puede agregar los archivos que respondan a estos criterios a una nueva categoría de aplicaciones. Más tarde, podrá usar esa nueva categoría para configurar el componente Control de aplicaciones.

Para crear una categoría de aplicaciones con contenido agregado manualmente:

1. En el menú principal, vaya a **Operaciones → Aplicaciones de terceros → Categorías de aplicaciones**.

   Se muestra una página con una lista de categorías de aplicaciones.

2. Haga clic en el botón **Añadir**.

   Se inicia el Asistente para crear nueva categoría. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En el paso **Seleccione el método de creación de la categoría**, seleccione la opción **Categoría con contenido añadido manualmente. Los datos de los archivos ejecutables se añaden manualmente a la categoría**.

4. En el paso **Condiciones**, haga clic en el botón **Añadir** para añadir un criterio de condición e incluir archivos en la categoría de creación.

5. En el paso **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. La condición de la categoría solo coincide con los archivos ejecutables que están firmados por el certificado especificado.

   - **Especificar la ruta a la aplicación (se admiten máscaras)**

     Seleccione esta opción para especificar la ruta a un archivo o carpeta del dispositivo cliente que contenga los archivos ejecutables que quiera agregar a la categoría de aplicaciones personalizada. Puede utilizar expresiones regulares como *C:\path_to_exe**, por ejemplo: *C:\Program Files\Internet Explorer**.

   - **Unidad extraíble**

     Seleccione esta opción para especificar el tipo de soporte (unidad extraíble o cualquier tipo de unidad) desde el que se ejecuta la aplicación. Las aplicaciones que se inicien desde el tipo de unidad seleccionado se agregarán a la categoría de aplicaciones personalizada.

   - **Hash, metadatos o certificado**:

     - **Seleccionar de la lista de archivos ejecutables**

       Seleccione esta opción si desea elegir las aplicaciones que se agregarán a la categoría de la lista de archivos ejecutables almacenados en el dispositivo cliente.

     - **Seleccionar del registro de aplicaciones**

Si selecciona esta opción, se abrirá el registro de aplicaciones. Después de seleccionar una aplicación del registro, se abre la ventana con los parámetros completados con metadatos de la aplicación que seleccionó:

- Nombre del archivo.
- Versión del archivo. Puede indicar el número de versión exacto o introducir una condición, como "superior a 5.0".
- Nombre de la aplicación.
- Versión de la aplicación. Puede indicar el número de versión exacto o introducir una condición, como "superior a 5.0".
- Proveedor.

Tenga en cuenta que solo se bloquea la ejecución de archivos ejecutables que cumplan con los parámetros especificados, no la ejecución de la aplicación que seleccione. Si los metadatos de la aplicación seleccionada coinciden con el del archivo ejecutable que se ejecuta al iniciar la aplicación, puede continuar con el siguiente paso. De lo contrario, debe cambiar los valores manualmente para que coincidan con los metadatos del archivo ejecutable.

- Especificar manualmente

Selecciona esta opción para especificar los metadatos, el certificado o el hash de archivo que se tomarán como condición para agregar aplicaciones a la categoría personalizada.

Hash del archivo

Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center Cloud Console calcule el valor de hash para archivos en esta categoría. La información sobre los valores hash calculados por las funciones hash se almacena en la base de datos del Servidor de administración.

SHA256 es una función de hash criptográfica. En la actualidad, se la considera la más fiable en su clase, pues no se ha encontrado vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security puede calcular hashes SHA256 desde la versión 10 Service Pack 2 para Windows. Las versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows son compatibles con la función de hash MD5.

Seleccione cualquiera de las opciones de cálculo del valor de hash de Kaspersky Security Center Cloud Console para archivos en la categoría:

- Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores, marque la casilla **SHA256**. Si hay versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows en su red, recomendamos que no añada categorías que utilicen como criterio el hash SHA256 del archivo ejecutable. Si lo hace, la aplicación de seguridad podría no funcionar correctamente. De presentarse inconvenientes, utilice la función de hash criptográfico MD5 para los archivos de la categoría.

- Si hay alguna versión anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows instalada en su red, seleccione **Hash MD5**. No puede agregar una categoría que se haya creado según el criterio de la suma de verificación MD5 de un archivo ejecutable para Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores. De presentarse inconvenientes, utilice la función de hash criptográfico SHA256 para los archivos de la categoría.

- Si diferentes dispositivos en su red usan versiones anteriores y posteriores de Kaspersky Endpoint Security 10, marque la casilla **SHA256** y la casilla **Hash MD5**.

Metadatos

Seleccione esta opción si desea especificar los metadatos de los archivos (nombre, versión, proveedor, etc.). La condición de la categoría solo coincide con los archivos ejecutables que tienen los mismos metadatos.

Certificado

Seleccione esta opción para elegir certificados almacenados en el repositorio. La condición de la categoría solo coincide con los archivos ejecutables que están firmados por el certificado especificado.

- Desde archivo o paquete MSI/carpeta archivada

Seleccione esta opción para especificar un archivo de instalador MSI como condición para agregar aplicaciones a la categoría personalizada. Los metadatos del instalador se enviarán al Servidor de administración. Las aplicaciones que tengan los mismos metadatos de instalador que el instalador MSI especificado se agregarán a la categoría de aplicaciones personalizada.

El criterio seleccionado se agrega a la lista de condiciones.

Puede agregar tantos criterios como necesite para crear la categoría de aplicaciones.

6. En el paso **Exclusiones**, haga clic en el botón **Añadir** para añadir un criterio de condición excluyente que permita excluir archivos de la nueva categoría.

7. En el paso **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 sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux

Crear una categoría de aplicaciones con archivos ejecutables de dispositivos específicos

Puede usar archivos ejecutables almacenados en ciertos dispositivos puntuales como modelo de los archivos ejecutables que quiera permitir o bloquear. Los archivos ejecutables de estos dispositivos pueden servirle de base para crear una categoría, que luego podrá usar en la configuración del componente Control de aplicaciones.

Para crear una categoría que incluya archivos ejecutables de dispositivos seleccionados:

1. En el menú principal, vaya a **Operaciones → Aplicaciones de terceros → Categorías de aplicaciones**.

   Aparece la página con una lista de categorías de archivos ejecutables.

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 el paso **Seleccione el método de creación de la categoría**, especifique el nombre para 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. 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 Cloud Console calcule el valor de hash para archivos en esta categoría. La información sobre los valores hash calculados por las funciones hash se almacena en la base de datos del Servidor de administración.

SHA256 es una función de hash criptográfica. En la actualidad, se la considera la más fiable en su clase, pues no se ha encontrado vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security puede calcular hashes SHA256 desde la versión 10 Service Pack 2 para Windows. Las versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows son compatibles con la función de hash MD5.

Seleccione cualquiera de las opciones de cálculo del valor de hash de Kaspersky Security Center Cloud Console para archivos en la categoría:

- Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores, marque la casilla **SHA256**. Si hay versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows en su red, recomendamos que no añada categorías que utilicen como criterio el hash SHA256 del archivo ejecutable. Si lo hace, la aplicación de seguridad podría no funcionar correctamente. De presentarse inconvenientes, utilice la función de hash criptográfico MD5 para los archivos de la categoría.

- Si hay alguna versión anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows instalada en su red, seleccione **Hash MD5**. No puede agregar una categoría que se haya creado según el criterio de la suma de verificación MD5 de un archivo ejecutable para Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores. De presentarse inconvenientes, utilice la función de hash criptográfico SHA256 para los archivos de la categoría.

Si diferentes dispositivos en su red usan versiones anteriores y posteriores de Kaspersky Endpoint Security 10, marque la casilla **SHA256** y la casilla **Hash MD5**.

La casilla **Calcular SHA256 para los archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)** está activada de 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 el asistente termina, se crea la categoría sobre archivos ejecutables. La nueva categoría aparece en la lista de categorías. Podrá usar la nueva categoría cuando configure Control de aplicaciones.

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**. Cuando el modo de prueba está habilitado, Kaspersky Endpoint Security para Windows no bloquea el inicio de las aplicaciones, pero registra información sobre las reglas activadas en el informe. Haga clic en el vínculo **Ver informe** para ver esa información.

6. Habilite la opción **Controlar la carga de módulos DLL** si desea que Kaspersky Endpoint Security para Windows monitoree la carga de módulos DLL cuando los usuarios inicien aplicaciones.

   Se guardará un informe con datos sobre los módulos y sobre las aplicaciones que carguen esos módulos.

   Kaspersky Endpoint Security para Windows 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 sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux

Agregar archivos ejecutables vinculados a eventos a una categoría de aplicaciones

Una vez que configure el componente Control de aplicaciones en las directivas de Kaspersky Endpoint Security para Windows, podrá ver los siguientes eventos en la lista de eventos:

- **Inicio de aplicación prohibido** (evento de nivel *Crítico*). Este evento se muestra si Control de aplicaciones se ha configurado para hacer cumplir sus reglas.
- **Inicio de aplicación prohibido en el modo de prueba** (evento de nivel *Información*). Este evento se muestra si Control de aplicaciones se ha configurado para aplicar sus reglas en modo de prueba.
- **Mensaje para el administrador sobre la prohibición de inicio de la aplicación** (evento de *advertencia*). Este evento aparece si Control de aplicaciones se ha configurado para hacer cumplir sus reglas y un usuario ha solicitado acceso a una aplicación que no tiene permitido ejecutar.

Recomendamos crear selecciones de eventos para ver los eventos relacionados con el funcionamiento de Control de aplicaciones.

Puede agregar los archivos ejecutables vinculados a los eventos de Control de aplicaciones a una categoría de aplicaciones nueva o existente. En cualquiera de los dos casos, la categoría debe ser una categoría de aplicaciones con contenido agregado manualmente.

Para agregar archivos ejecutables vinculados a los eventos de Control de aplicaciones a una categoría de aplicaciones:

1. En el menú principal, vaya a **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 SHA256 para archivos sin certificado)

    Los archivos pueden estar firmados con un certificado. Cada certificado puede utilizarse para firmar más de un archivo. Un mismo certificado puede usarse para firmar distintas versiones de una misma aplicación, por ejemplo, o distintas aplicaciones de un mismo proveedor. Cuando seleccione un certificado, podría suceder que la categoría termine con varias versiones de una misma aplicación o con varias aplicaciones de un mismo proveedor.

    Cada archivo tiene su propia función hash SHA256. Si selecciona una función hash SHA256, solo se añadirá a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

    Seleccione esta opción si desea añadir los detalles del certificado de un archivo ejecutable (o la función hash SHA256 de los archivos sin certificado) a las reglas de la categoría.

    Esta opción está seleccionada de 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 SHA256 (se omitirán los archivos sin hash)**

  Cada archivo tiene su propia función hash SHA256. Si selecciona una función hash SHA256, solo se añadirá a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

  Seleccione esta opción si solo desea añadir los detalles de la función hash SHA256 del archivo ejecutable.

- **Solo MD5 (modo discontinuado, solo para Kaspersky Endpoint Security 10 Service Pack 1)**

  Cada archivo tiene su propia función hash MD5. Si selecciona una función hash MD5, solo se agregará a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

  Seleccione esta opción si solo desea agregar los detalles de la función hash MD5 del archivo ejecutable. La capacidad de calcular hashes MD5 está disponible para Kaspersky Endpoint Security 10 Service Pack 1 para Windows y versiones anteriores.

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 sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux

Crear un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky

Kaspersky Security Center Web Console le permite realizar la instalación remota de aplicaciones de terceros mediante el uso de paquetes de instalación. Estas aplicaciones de terceros se incluyen en una base de datos dedicada de Kaspersky.

Crear paquetes de instalación de aplicaciones de terceros desde la base de datos de Kaspersky solo está disponible bajo la licencia de Administración de vulnerabilidades y parches.

Para crear un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky, haga lo siguiente:

1. En el menú principal, vaya a **Detección y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**.
2. Haga clic en el botón **Añadir**.
3. En la página del Asistente de nuevo paquete que se abre, seleccione la opción **Seleccionar una aplicación de la base de datos de Kaspersky para crear un paquete de instalación** y luego haga clic en **Siguiente**.
4. En la lista de aplicaciones que se abre, seleccione la aplicación correspondiente y luego haga clic en **Siguiente**.
5. Seleccione el idioma de localización relevante en la lista desplegable y luego haga clic en **Siguiente**.

   Este paso solo se muestra si la aplicación brinda varias opciones de idiomas.

6. Si se le solicita que acepte un Acuerdo de licencia para la instalación, en la página **Contrato de licencia de usuario final** que se abre, haga clic en el vínculo para leer el Contrato de licencia en el sitio web del proveedor y luego seleccione la casilla de verificación **Confirmo que he leído, entiendo y acepto en su totalidad los términos y condiciones de este Contrato de licencia de usuario final**.
7. En la página **Nombre del nuevo paquete de instalación** que se abre, en el campo **Nombre del paquete**, ingrese el nombre del paquete de instalación y luego haga clic en **Siguiente**.

Espere hasta que el paquete de instalación recién creado se cargue en el Servidor de administración. Cuando el Asistente de nuevo paquete muestre el mensaje que le informa que el proceso de creación del paquete se creó con éxito, haga clic en **Finalizar**.

El paquete de instalación recién creado aparecerá en la lista de paquetes de instalación. Puede seleccionar este paquete al crear o reconfigurar la tarea *Instalar aplicación de forma remota*.

Ver y modificar la configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky

Si creó previamente algún paquete de instalación de aplicaciones de terceros incluidas en la base de datos de Kaspersky, podrá ver y modificar posteriormente la configuración de estos paquetes.

La modificación de la configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky solo está disponible bajo la licencia de Administración de vulnerabilidades y parches.

Para ver y modificar la configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky:

1. En el menú principal, vaya a **Detección y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**.
2. En la lista de paquetes de instalación que se abre, haga clic en el nombre del paquete correspondiente.
3. En la página de propiedades que se abre, modifique la configuración, si es necesario.
4. Haga clic en el botón **Guardar**.

Se guardará la configuración que modificó.

Configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky

La configuración de un paquete de instalación de una aplicación de terceros se agrupa en las siguientes pestañas:

Solo una parte de la configuración que se muestra a continuación se muestra de forma predeterminada, por lo que puede agregar las columnas correspondientes haciendo clic en **Filtro** y seleccionando los nombres de columna relevantes de la lista.

- Pestaña **General**:
  - Campo de entrada que contiene el nombre del paquete de instalación que se puede editar manualmente
  - Aplicación

    El nombre de la aplicación de terceros para la que se crea el paquete de instalación.
  - Versión

    El número de versión de la aplicación de terceros para la que se creó el paquete de instalación.
  - Tamaño

    El tamaño del paquete de instalación de terceros (en kilobytes).
  - Creado

    La fecha y la hora en que se creó el paquete de instalación de terceros.
  - Ruta

    La ruta a la carpeta de red donde se almacena el paquete de instalación de terceros.
- Pestaña **Proceso de instalación**:
  - Instalar los componentes generales del sistema necesarios

    Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Por ejemplo, estos requisitos previos pueden ser actualizaciones del sistema operativo.

    Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

    Esta opción está deshabilitada de manera predeterminada.
  - Tabla que muestra las propiedades de actualización y que contiene las siguientes columnas:

- **Nombre**

  Nombre de la actualización.

- **Descripción**

  Descripción de la actualización.

- **Origen**

  La fuente de la actualización, es decir, si la lanzó Microsoft o un desarrollador externo diferente.

- **Tipo**

  El tipo de actualización, es decir, si está destinada a un controlador o una aplicación.

- **Categoría**

  La categoría de Windows Server Update Services (WSUS) que se muestra para las actualizaciones de Microsoft (Actualizaciones críticas, Actualizaciones de las definiciones, Controladores, Paquetes de características, Actualizaciones de seguridad, Service Packs, Herramientas, Paquetes acumulativos de actualizaciones, Actualizaciones o Actualización).

- **Nivel de importancia según MSRC**

  El nivel de importancia de la actualización definido por Microsoft Security Response Center (MSRC).

- **Nivel de importancia**

  El nivel de importancia de la actualización definido por Kaspersky.

- **Nivel de importancia del parche**

  El nivel de importancia del parche si está destinado para una aplicación de Kaspersky.

- **Artículo**

  El identificador (id.) del artículo de la Base de conocimientos que describe la actualización.

- **Boletín**

  El id. del boletín de seguridad que describe la actualización.

- **No asignada para instalación (nueva versión)**

  Muestra si la actualización tiene el estado Instalación no asignada.

- **Para instalar**

Muestra si la actualización tiene el estado Por instalarse.

- **Instalando**

  Muestra si la actualización tiene el estado Instalando.

- **Instalada**

  Muestra si la actualización tiene el estado Instalada.

- **Error**

  Muestra si la actualización tiene el estado Error.

- **Se requiere reiniciar**

  Muestra si la actualización tiene el estado Se debe reiniciar el dispositivo.

- **Registrada**

  Muestra la fecha y hora en que se registró la actualización.

- **Se ha instalado en modo interactivo**

  Muestra si la actualización solicita una interacción con el usuario durante la instalación.

- **Anulado**

  Muestra la fecha y hora en que se revocó la actualización.

- **Estado de aprobación de la actualización**

  Muestra si la actualización está aprobada para su instalación.

- **Revisión**

  Muestra el número de revisión actual de la actualización.

- **Id. de actualización**

  Muestra el id. de la actualización.

- **Versión de la aplicación**

  Muestra el número de versión a la que se actualizará la aplicación.

- **Sustituido**

Muestra otras actualizaciones que pueden reemplazar a la actualización.

- **Sustituyendo**

  Muestra otras actualizaciones que pueden ser reemplazadas por la actualización.

- **Debe aceptar las condiciones del Contrato de licencia**

  Muestra si la actualización solicita la aceptación de los términos de un Contrato de licencia de usuario final (EULA).

- **Dirección de URL de la descripción**

  Muestra el nombre del proveedor de la actualización.

- **Familia de la aplicación**

  Muestra el nombre de la familia de aplicaciones a las que pertenece la actualización.

- **Aplicación**

  Muestra el nombre de la aplicación a la que pertenece la actualización.

- **Idioma de localización**

  Muestra el idioma de la localización de la actualización.

- **No asignada para instalación (nueva versión)**

  Muestra si la actualización tiene el estado Instalación no asignada (nueva versión).

- **Requiere la instalación de requisitos previos**

  Muestra si la actualización tiene el estado Requiere instalación de requisitos previos.

- **Modo de descarga**

  Muestra el modo de descarga de la actualización.

- **Es un parche**

  Muestra si la actualización es un parche.

- **No instalado**

  Muestra si la actualización tiene el estado Sin instalar.

- Pestaña **Configuración** que muestra la configuración del paquete de instalación (con sus nombres, descripciones y valores) que se utilizan como parámetros de la línea de comandos durante la instalación. Si el paquete no proporciona dicha configuración, se muestra el mensaje correspondiente. Puede modificar los valores de esta configuración.

- Pestaña **Historial de revisión** que muestra las revisiones del paquete de instalación y que contiene las siguientes columnas:

  - **Revisión**: muestra el número de revisión de los paquetes de instalación.

  - **Hora** fecha y hora de modificación de la configuración del paquete de instalación.

  - **Usuario** nombre del usuario que modificó la configuración del paquete de instalación.

  - **Acción** acción realizada sobre el paquete de instalación dentro de la revisión.

  - **Descripción** descripción de la revisión vinculada al cambio realizado en la configuración del paquete de instalación.

    De forma predeterminada, la descripción de las revisiones está en blanco. Para agregar una descripción a una revisión, seleccione la revisión pertinente y haga clic en el botón **Editar descripción**. En la ventana abierta, ingrese el texto que describa la revisión.

Etiquetas de aplicación

Kaspersky Security Center Cloud Console le permite etiquetar las aplicaciones desde el registro de aplicaciones. Las etiquetas son rótulos que se asignan a las aplicaciones y que pueden utilizarse para agruparlas o encontrarlas. Asignada a una serie de aplicaciones, una etiqueta puede servir de condición para crear una selección de dispositivos.

Por ejemplo, puede crear la etiqueta `[Navegadores]` y asignarla a todos los navegadores, como Microsoft Internet Explorer, Google Chrome y Mozilla Firefox.

Creación de una etiqueta de aplicación

Para crear una etiqueta de aplicación:

1. En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Etiquetas de aplicaciones**.

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 aplicaciones**.
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 aplicaciones**.

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.

Configuración del Servidor de administración

Esta sección describe el proceso de configuración y las propiedades del Servidor de administración de Kaspersky Security Center.

Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario

Puede hacer que un Servidor de administración en ejecución in situ funcione como Servidor de administración secundario y, así, establecer una jerarquía "principal/secundario" en su red. Para el Servidor de administración que se encuentra en la infraestructura de Kaspersky, los Servidores de administración principal y secundario en su red son ambos servidores secundarios. Puede agregar un Servidor de administración basado en Windows, así como un Servidor de administración basado en Linux.

Para añadir un Servidor de administración secundario que se pueda conectar, realice lo siguiente:

1. Asegúrese de que el Servidor de administración secundario futuro tenga instalado Kaspersky Security Center Web Console.

2. En el Servidor de administración secundario futuro, descargue el certificado del Servidor de administración y guárdelo para poder añadirlo al Servidor de administración principal en uno de los pasos del Asistente para añadir un Servidor de administración secundario.

3. Realice las siguientes acciones a través de Kaspersky Security Center Web Console en el Servidor de administración secundario futuro (también puede solicitar que el administrador del Servidor de administración secundario futuro realice estas acciones):

   a. En el menú principal, haga clic en el icono de configuración ( ) junto al nombre del futuro Servidor de administración secundario.

   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. Seleccione **Cloud Console** como el tipo del Servidor de administración principal.

      Los campos de configuración para establecer una conexión entre los Servidores de administración secundario y primario se vuelven disponibles.

   e. En los campos **Dirección del Servidor HDS (del Servidor de administración principal en Cloud Console)** y **Puertos del servidor HDS**, introduzca la dirección y el puerto del Servidor de administración principal de Kaspersky Security Center Cloud Console.

      Puede encontrar la dirección del servidor HDS y el puerto del servidor HDS en el Servidor de administración de Kaspersky Security Center Cloud Console, en la sección **Jerarquía de Servidores de administración** de la pestaña **General** en la ventana de propiedades. Puede copiar y pegar esta información en los campos de la ventana del Servidor de administración secundario.

   f. Haga clic en el botón **Especificar el certificado del Servidor de administración principal** y, luego, seleccione el certificado.

      Puede descargar este certificado desde el Servidor de administración de Kaspersky Security Center Cloud Console en la sección **Jerarquía de Servidores de administración** de la pestaña **General** en la ventana de propiedades haciendo clic en el botón **Ver certificado del Servidor de administración**.

g. Haga clic en el botón **Especificar certificados del servicio Hosted Discovery Service**, y luego seleccione el certificado.

Puede descargar este certificado desde el Servidor de administración de Kaspersky Security Center Cloud Console, en la sección **Jerarquía de Servidores de administración** de la pestaña **General** de la ventana de propiedades, haciendo clic en el botón **Certificado CA de origen HDS**.

h. Si utiliza un servidor proxy para conectarse al Servidor de administración de Kaspersky Security Center Cloud Console (es decir al Servidor principal en la jerarquía que ha creado), especifíquelo e introduzca las credenciales del servidor proxy.

i. Seleccione la opción **Conectar Servidor de administración principal a Servidor de administración secundario en DMZ** si el Servidor de administración secundario está en una zona desmilitarizada.

j. Haga clic en **Guardar** para guardar los cambios y salir de la ventana.

4. En el menú principal, haga clic en el icono de configuración ( ) junto al nombre del futuro Servidor de administración principal.

5. En la página de propiedades que se abre, haga clic en la pestaña **Servidores de administración**.

6. Seleccione la casilla de verificación junto al nombre del grupo de administración al que desea añadir el Servidor de administración secundario.

7. En la línea del menú, haga clic en **Conectar Servidor de administración secundario**.

Se inicia el Asistente para añadir un Servidor de administración secundario. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

8. Rellene 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.

  Este parámetro es obligatorio si está activada la opción **Conectar el Servidor de administración principal al Servidor de administración secundario en DMZ**.

9. Si utiliza un servidor proxy para conectarse al Servidor de administración de Kaspersky Security Center Cloud Console (es decir, al futuro Servidor principal), especifíquelo e introduzca las credenciales del servidor proxy.

10. Siga las instrucciones adicionales del asistente.

Una vez que el asistente termina, se crea la jerarquía "principal/secundario". El Servidor de administración principal empieza a aceptar conexiones del Servidor de administración secundario utilizando el puerto 13000. Se recibirán y aplicarán las tareas y directivas del Servidor de administración principal. El Servidor de administración secundario aparecerá en el Servidor de administración principal, en el grupo de administración en el que se lo haya agregado.

Configuración del plazo de almacenamiento de eventos relacionados con los dispositivos eliminados

En Kaspersky Security Center Cloud Console, los eventos se almacenan en un repositorio de eventos. No puede configurar cuántos eventos se almacenan en el repositorio de eventos.

En la sección **Repositorio de eventos** de la ventana de propiedades del Servidor de administración, puede configurar el plazo máximo de almacenamiento de eventos relacionados con los dispositivos eliminados. El plazo de almacenamiento máximo es de 1000 días.

Para configurar por cuantos días se almacenarán los eventos relacionados con los dispositivos eliminados:

1. En el menú principal, haga clic en el icono de configuración ( ) junto al Servidor de administración de Kaspersky Security Center Cloud Console.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la ficha **General**, seleccione la sección **Repositorio de eventos**.

3. Habilite la opción **Almacenar eventos tras la eliminación de los dispositivos**.

4. En el cuadro de edición **Periodo máximo de almacenamiento (días)** especifique el número de días que se almacenarán los eventos relacionados con los dispositivos eliminados.

   El número de días que se almacenarán los eventos relacionados con los dispositivos eliminados se limita por el valor especificado.

Además, puede cambiar la configuración de cualquier tarea para guardar eventos relacionados con el progreso de la misma, o guardar solo los resultados de la ejecución de la tarea. Al hacerlo, reducirá la cantidad de eventos en la base de datos, aumentará la velocidad de ejecución de los escenarios asociados con el análisis de la tabla de eventos en la base de datos y disminuirá el riesgo de que una gran cantidad de eventos sobrescriban eventos críticos.

Agrupación de mensajes de correo electrónicos sobre eventos

Durante la operación, Kaspersky Security Center Cloud Console y las aplicaciones de Kaspersky administradas generan eventos. Cada evento se atribuye a un determinado tipo y nivel de gravedad (*Crítico*, *Fallo operativo*, *Advertencia* o *Información*). Según las condiciones en que tengan lugar los eventos, Kaspersky Security Center Cloud Console puede asignar diferentes niveles de gravedad a eventos del mismo tipo.

Kaspersky Security Center Cloud Console envía notificaciones sobre eventos automáticamente, por correo electrónico. Kaspersky Security Center Cloud Console envía notificaciones sobre los eventos enumerados en la ventana **Propiedades del Servidor de administración** en la pestaña **Configuración de eventos**. La configuración de notificación común se utiliza para todos los tipos de eventos.

Para limitar el número de correos electrónicos que deben enviarse, Kaspersky Security Center Cloud Console, agrega eventos con el mismo nivel de gravedad durante periodos específicos. Los especialistas de Kaspersky administran los valores de los periodos. Como resultado, los destinatarios reciben mensajes de correos electrónicos agregados conforme a la siguiente plantilla: "Se produjeron <número> eventos <nivel_de_gravedad> (y de un nivel inferior)".

Limitaciones en la administración de Servidores de administración secundarios que se ejecutan de forma local a través de Kaspersky Security Center Cloud Console

Después de cambiar a un Servidor de administración secundario que se ejecuta de forma local mediante la opción correspondiente en Kaspersky Security Center Cloud Console, la aplicación impone limitaciones específicas en la administración de este Servidor de administración secundario. Las siguientes configuraciones relacionadas con la operación de Kaspersky Security Center Cloud Console no estarán disponibles para el usuario:

- En la configuración de las directivas del Agente de red y del Servidor de administración, las pestañas **Configuración de eventos** y **Configuración de la aplicación** no están disponibles. No se pueden crear directivas nuevas.
- En la configuración de las tareas del Agente de red y del Servidor de administración, las pestañas **Configuración de eventos** y **Configuración de la aplicación** no están disponibles. No se pueden crear tareas nuevas.
- La administración del Agente de red y el Servidor de administración no está disponible, así como la ventana de propiedades del Servidor de administración secundario.
- El asistente de inicio rápido no está disponible.
- La configuración de almacenamiento y notificación para los eventos del Agente de red y el Servidor de administración no se puede modificar.
- La sección **Versiones actuales de la aplicación** no está disponible.
- La sección **Paquetes de instalación** no está disponible.

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.

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.

Configuración de la interfaz

Puede configurar la interfaz de Kaspersky Security Center Cloud Console para mostrar y ocultar secciones y elementos de la interfaz, según las funciones que utilice.

Para configurar la interfaz de Kaspersky Security Center Cloud Console de acuerdo con el conjunto de funciones utilizado actualmente:

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 las opciones:
   - **Mostrar protección y cifrado de datos**

     Puede utilizar esta opción para ocultar o mostrar la sección **Operaciones → Protección y cifrado de datos** en la interfaz. Kaspersky Security Center Cloud Console guarda el valor de esta opción solo para su propia cuenta de usuario. Otro usuario puede establecer un valor diferente.

   - **Mostrar las funciones de MDR**

     Puede utilizar esta opción para ocultar o mostrar la sección **Control e informes → Incidentes** en la interfaz. Kaspersky Security Center Cloud Console guarda el valor de esta opción solo para su propia cuenta de usuario. Otro usuario puede establecer un valor diferente.
3. Establezca la cantidad de dispositivos que Kaspersky Security Center Cloud Console muestra en los resultados de distribución de directivas.
4. Haga clic en **Guardar**.

La configuración de la interfaz de la consola se configura según sus preferencias.

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.
4. En la línea del menú, haga clic en **Nuevo Servidor de administración virtual**.
5. En la página que se abre, defina el **Nombre del Servidor de administración virtual**.
6. 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**.

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 esté incluido en la lista **Derechos de acceso** en las propiedades del 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

Cuando asigne un administrador, asegúrese de conceder acceso a un solo Servidor de administración virtual. Un administrador con acceso a varios Servidores de administración virtuales no puede iniciar sesión en Kaspersky Security Center Cloud Console.

Un administrador de un Servidor de administración virtual inicia sesión en Kaspersky Security Center Cloud Console de la misma manera que inicia sesión en el Servidor de administración principal. Kaspersky Security Center Cloud 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.
- La cuenta creada del administrador del servidor virtual no está incluida en las listas de **Derechos de acceso** de las propiedades de cualquier servidor, principal o secundario.
- 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.

Al asignar funciones a un usuario, en el menú principal, vaya a **Usuarios y funciones** → **Usuarios y grupos** y, luego, seleccione la pestaña **Usuarios**. Si selecciona la pestaña **Grupos** y, luego, asigna funciones al grupo en el que el usuario es miembro, el usuario no podrá iniciar sesión en Kaspersky Security Center Cloud Console.

La aplicación asigna la nueva función 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.

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 bajo la administración de Kaspersky Security Center Cloud Console, 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.

Supervisión e informes

Esta sección describe las capacidades de supervisión e informes de Kaspersky Security Center Cloud Console. 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 Cloud Console o durante la 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 Cloud Console.

Requisitos previos

Después de desplegar Kaspersky Security Center Cloud Console en la red de una organización, puede comenzar a supervisarlo y generar informes sobre su funcionamiento.

Etapas

La configuración de la supervisión y la elaboración de informes en la red de una organización se realiza 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 esta configuración, puede cambiar la cantidad de eventos con niveles de importancia Crítico 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: configurar notificaciones (por correo electrónico) de eventos en dispositivos cliente

3. **Cambiar el modo en que la red de seguridad responde al evento Brote de virus**

   Puede modificar los umbrales específicos en las propiedades del Servidor de administración. También puede crear una directiva más estricta que se active cuando ocurra este evento (o una tarea que se ejecute cuando ocurra este evento).

4. **Controlar el estado de seguridad de la red de la organización**

   Instrucciones:

   - Revise el widget **Estado de la protección**
   - Genere y revise el **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:

   - Genere y revise los informes de las categorías **Estado de la protección** y **Estadísticas de amenazas**
   - Inicie y revise la selección de **Crítico**

7. **Controlar la información de las licencias**

   Instrucciones:

   - Añada el widget de **Uso de claves de licencia** al panel y revíselo
   - 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 Cloud Console proporciona los siguientes tipos de monitoreo e informes en la red de su organización:

- Panel
- Informes
- Selecciones de eventos

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 crear y ver selecciones de eventos definidos por el usuario según la configuración disponible en la interfaz de Kaspersky Security Center Cloud Console para configurarlas.

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.

El panel de control está disponible en Kaspersky Security Center Cloud Console, en la sección **Control e informes**, al hacer clic en **Panel**.

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 Cloud 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 Cloud Console (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 del usuario, para que pueda realizar varias acciones en Kaspersky Security Center Cloud Console, 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 Cloud Console 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.

Los informes están disponibles en Kaspersky Security Center Cloud Console, en la sección **Control e informes**, al hacer clic en **Informes**.

Por defecto, los informes contienen información de los últimos treinta días.

Kaspersky Security Center Cloud Console 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**.
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. Introduzca el nombre del informe y seleccione el tipo de informe.
4. En el paso **Cobertura** del asistente, seleccione el conjunto de dispositivos cliente (grupo de administración, selección de dispositivos, dispositivos seleccionados o todos los dispositivos de red) cuyos datos se mostrarán en informes que se basen en esta plantilla de informe.
5. En el paso **Período del informe**, especifique el período del informe. Los valores disponibles son los siguientes:

   - Entre dos fechas específicas
   - Desde una fecha específica hasta la fecha de creación del informe
   - Desde cierta cantidad de días antes de la creación del informe hasta la fecha de creación del informe

   Esta página puede no aparecer para algunos informes.
6. Haga clic en **Aceptar** para cerrar el asistente.
7. Realice una de las siguientes acciones:

   - Haga clic en el botón **Guardar y ejecutar** para guardar la nueva plantilla de informe y crear un informe basado en ella.

     Se guardará la plantilla de informe. Se generará el informe.
   - Haga clic en el botón **Guardar** para guardar la nueva plantilla de informe.

     Se guardará la plantilla de informe.

Puede utilizar la nueva plantilla para generar y ver informes.

Ver y editar las propiedades de una plantilla de informe

Puede ver y editar las propiedades básicas de las plantillas de informe (por ejemplo, el nombre de las plantillas o los campos que se muestran en los informes).

Para ver y editar las propiedades de una plantilla de informe:

1. En el menú principal, vaya a **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.

    Tenga en cuenta que la interfaz de Kaspersky Security Center Cloud Console puede mostrar un máximo de 2500 entradas. Si necesita ver un número mayor de eventos, utilice la función exportación de informes.

  - **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 Cloud Console 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 abierta, especifique 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.

   - **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.

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 solo en inglés, no se dispone de otras localizaciones.

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. 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 **Crear tarea de entrega**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
4. En el paso **Configuración de tarea nueva** del asistente, introduzca el nombre de la tarea.

   El nombre predeterminado es **Entregar informes**. Si ya existe una tarea con este nombre, se añade un número de secuencia (<N>) al nombre de la tarea.

5. En el paso **Configuración del informe** del asistente, especifique la siguiente configuración:

   a. Seleccione las plantillas de informe que entregará la tarea.

   b. Defina el formato de los informes: HTML, XLS o PDF.

      Se requiere la herramienta wkhtmltopdf para convertir un informe a PDF. Cuando selecciona la opción PDF, el Servidor de administración verifica si la herramienta wkhtmltopdf está instalada en el dispositivo. Si la herramienta no está instalada, la aplicación muestra un mensaje sobre la necesidad de instalar la herramienta en el dispositivo del Servidor de administración. Instale la herramienta manualmente y luego continúe con el siguiente paso.

   c. Indique si los informes se enviarán por correo electrónico y, de ser así, defina los ajustes de notificación por correo electrónico.

      Puede especificar hasta 20 direcciones de correo electrónico. Para separar direcciones de correo electrónico, presione **Intro**. También puede pegar una lista de direcciones de correo electrónico separadas por comas y, luego, presionar **Intro**.

6. En el paso **Configurar programación de tareas** del asistente, seleccione la programación de inicio de la tarea.

   Están disponibles las siguientes opciones de programación de tareas:

   - Manualmente

     La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

     Esta opción está seleccionada 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 manera 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.

- **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.

- **En los días especificados**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  De manera predeterminada, no se selecciona ningún día del mes. La hora de inicio predeterminada es a las 18:00.

- **Al detectar un brote de virus**

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completar otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. Este parámetro solo funciona si ambas tareas están asignadas a los mismos dispositivos. Por ejemplo, podría ejecutar la tarea *Administrar dispositivos* con la opción **Encender dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Se completó correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Introduzca el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el icono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el icono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

7. En este paso del asistente, configure otras opciones de programación de tareas:

- En la sección **Programación de la tarea**, verifique o reconfigure la programación previamente seleccionada y establezca el intervalo de tiempo, los días del mes o la semana, establezca la condición de brote de virus o la finalización de otra tarea como disparador para iniciar la tarea. También se puede especificar una hora de inicio en esta sección si se selecciona una programación aplicable.

- En la sección **Configuración adicional**, especifique las siguientes configuraciones:

  - Ejecutar tareas no realizadas

    Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

    Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **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 las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manualmente**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

    Esta opción está deshabilitada de manera predeterminada.

  - Usar el retraso aleatorio automáticamente para el inicio de la tarea

    Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

    La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

    Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  - Usar el retraso aleatorio automáticamente para el inicio de la tarea con un intervalo de

    Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

    Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

    Esta opción está deshabilitada de manera predeterminada. El intervalo de tiempo predeterminado es de un minuto.

  - Detener la tarea si tarda más de

Una vez que transcurra el período especificado, la tarea se detendrá automáticamente, se haya completado o no.

Habilite esta opción si desea que las tareas que tarden mucho en completarse se interrumpan o se detengan.

Esta opción está deshabilitada de manera predeterminada. El tiempo de ejecución por defecto para las tareas es de 120 minutos.

8. En el paso **Seleccionar una cuenta para ejecutar la tarea** del asistente, especifique las credenciales de la cuenta de usuario que se utiliza para ejecutar la tarea.

9. Si desea modificar otros valores de configuración de la tarea después de crear la tarea, en el paso **Finalizar la creación de tareas** del asistente, active la opción **Abrir los detalles de la tarea cuando se complete la creación** (esta opción está activada de manera predeterminada).

10. Haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

    Se creará la tarea de entrega de informes. Si la opción **Abrir los detalles de la tarea cuando se complete la creación** está habilitada, se abrirá la ventana de configuración de la tarea.

Eliminación de plantillas de informes

Para eliminar una o varias plantillas de informes:

1. En el menú principal, vaya a **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 Cloud Console y sobre cómo administrar el bloqueo de eventos frecuentes.

Acerca de los eventos de Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console le permite recibir información sobre los eventos de funcionamiento del Servidor de administración y aplicaciones de Kaspersky instaladas en dispositivos administrados. La información sobre estos eventos se guarda en la base de datos del Servidor de administración. Puede exportar esta información a un sistema SIEM externo. La exportación de la información de eventos a sistemas SIEM externos permite a los administradores de sistemas SIEM responder lo antes posible a eventos del sistema de seguridad que ocurren en dispositivos administrados o grupos de dispositivos.

Eventos por tipo

En Kaspersky Security Center Cloud Console 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 Cloud Console.
  - 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 *Fallo operativo* 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 Cloud Console. 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 Cloud Console

Cada componente de Kaspersky Security Center Cloud Console 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 Cloud Console. 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 Cloud Console 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 Cloud Console.
- **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.

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 Cloud Console 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	Una vez al día, Kaspersky Security Center Cloud Console comprueba si se excede una restricción de licencia. Este tipo de evento ocurre cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en los dispositivos cliente han superado algún límite de sus licencias y se ha utilizado más de un 110 % del total de unidades con licencia cubiertas por una sola licencia. Los dispositivos cliente se mantienen protegidos aun cuando ocurre este evento. Puede responder al evento de los siguientes modos: • Revise la lista de dispositivos administrados. Elimine los dispositivos que no estén en uso. • Agregue una licencia para más dispositivos (agregue un código de activación válido o un archivo de clave en el Servidor de administración). Kaspersky Security Center Cloud Console determina las reglas para generar eventos cuando se excede el límite de una licencia.	180 días
Brote de virus	26 (para Protección contra archivos peligrosos)	GNRL_EV_VIRUS_OUTBREAK	Los eventos de este tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto período de tiempo. Puede responder al evento de los siguientes modos: • Configure el umbral en las propiedades del Servidor de administración. • Cree una directiva más estricta que se active cuando ocurra este evento (o, como alternativa, cree una tarea que se ejecute cuando ocurra el evento).	180 días
Brote de virus	27 (para Protección contra amenazas de correo)	GNRL_EV_VIRUS_OUTBREAK	Los eventos de este tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto período de tiempo. Puede responder al evento de los siguientes modos: • Configure el umbral en las propiedades del Servidor de administración. • Cree una directiva más estricta que se active cuando ocurra este evento (o,	180 días

			como alternativa, cree una tarea que se ejecute cuando ocurra el evento).	
Brote de virus	28 (para el firewall)	GNRL_EV_VIRUS_OUTBREAK	Los eventos de este tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto período de tiempo. Puede responder al evento de los siguientes modos: • Configure el umbral en las propiedades del Servidor de administración. • Cree una directiva más estricta que se active cuando ocurra este evento (o, como alternativa, cree una tarea que se ejecute cuando ocurra el evento).	180 días
Se ha perdido la conexión con el dispositivo	4111	KLSRV_HOST_OUT_CONTROL	Este tipo de eventos ocurren si un dispositivo administrado es visible en la red pero no se ha conectado al Servidor de administración durante un período específico. Averigüe qué impide el correcto funcionamiento del Agente de red en el dispositivo. El problema podría deberse a un inconveniente en la red, por ejemplo, o al hecho de que el Agente de red se haya eliminado del dispositivo.	180 días
El estado del dispositivo es Crítico	4113	KLSRV_HOST_STATUS_CRITICAL	Este tipo de evento ocurre cuando se le asigna el estado *Crítico* a un dispositivo administrado. Puede configurar las condiciones bajo las cuales el estado del dispositivo cambia a *Crítico*.	180 días
Modo de funcionalidad limitada	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Los eventos de este tipo ocurren cuando Kaspersky Security Center Cloud Console empieza a funcionar con funcionalidad básica, sin la Administración de vulnerabilidades y parches y sin la función Administración de dispositivos móviles. Las causas de este evento y las maneras de responder son las siguientes: • El periodo de vigencia de la licencia ha caducado. Proporcione una licencia para utilizar el modo de funcionalidad completa de Kaspersky Security Center Cloud Console (añada un código de activación válido o un archivo clave al Servidor de administración). • El Servidor de administración gestiona más dispositivos de los que permite el límite de la licencia. Mueva los dispositivos de los grupos de administración de un Servidor de administración a los grupos de administración de otro Servidor de administración (si el límite de licencia del otro Servidor de administración lo admite).	180 días
La licencia caduca pronto	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Este tipo de evento ocurre cuando se acerca la fecha de caducidad de una licencia comercial.	180 días

			Kaspersky Security Center verifica una vez al día si alguna licencia está próxima a caducar. Los eventos de este tipo se publican 30 días, 15 días, 5 días y 1 día antes de la fecha de caducidad de la licencia. 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. Cuando caduca la licencia comercial, Kaspersky Security Center Cloud Console presta solo la funcionalidad básica. Puede responder al evento de los siguientes modos: • Asegúrese de tener una clave de licencia de reserva añadida en el Servidor de administración. • Si usa una suscripción, no olvide renovarla. Una suscripción ilimitada se renueva automáticamente si el proveedor de servicios recibe a término y por adelantado el pago correspondiente.	
El certificado de MDM ha caducado	4132	KLSRV_CERTIFICATE_EXPIRED	Este tipo de evento ocurre cuando caduca el certificado del Servidor de administración para Administración de dispositivos móviles. Deberá actualizar el certificado caducado.	180 días
Se han anulado las actualizaciones para los módulos de la aplicación de Kaspersky	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Este tipo de evento ocurre cuando los especialistas técnicos de Kaspersky revocan una actualización sin interrupciones (tales actualizaciones tienen el estado *Revocada*) y resulta necesario, por ejemplo, actualizar a una versión más nueva. El evento afecta a los parches de Kaspersky Security Center Cloud Console pero no a los módulos de las aplicaciones administradas de Kaspersky. La razón por la que no se instaló la actualización sin interrupciones se indica en el evento.	180 días
Auditoría: la exportación a SIEM produjo un error	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Los eventos de este tipo ocurren cuando la exportación de eventos al sistema SIEM falla debido a un error de conexión con el sistema SIEM.	180 días

Eventos del Servidor de administración: nivel Fallo operativo

La siguiente tabla muestra los eventos del Servidor de administración de Kaspersky Security Center Cloud Console 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 Fallo operativo

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 instalaciones para uno de los grupos de aplicaciones con licencia	4126	KLSRV_INVLICPROD_EXCEDED	El Servidor de administración genera eventos de este tipo periódicamente (cada una hora). Los eventos de este tipo ocurren si administra claves de licencia de aplicaciones de terceros en Kaspersky Security Center Cloud Console y si el número de instalaciones ha superado el límite establecido por la clave de licencia de la aplicación de terceros. Puede responder al evento de los siguientes modos: • Revise la lista de dispositivos administrados. Si la aplicación del tercero no se está utilizando en algún dispositivo, desinstálela de ese equipo. • Solicite al tercero una licencia para más dispositivos. Para administrar las claves de licencia de sus aplicaciones de terceros, puede utilizar la característica de grupos de aplicaciones con licencia. Un grupo de aplicaciones con licencia está formado por aplicaciones de terceros que cumplen con los criterios que usted define.	180 días
No se ha podido sondear el segmento de la nube	4143	KLSRV_KLCLOUD_SCAN_ERROR	Los eventos de este tipo ocurren cuando el Servidor de administración no puede sondear un segmento de red en un entorno de nube. Lea los detalles en la descripción del evento y responda en consecuencia.	No se almacena

Eventos del Servidor de administración: nivel Advertencia

La siguiente tabla muestra los eventos del Servidor de administración de Kaspersky Security Center Cloud Console 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 superado el límite de licencias	4098	KLSRV_EV_LICENSE_CHECK_100_110	Una vez al día, Kaspersky Security Center Cloud Console comprueba si se excede una restricción de licencia. Este tipo de evento ocurre cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en los dispositivos cliente han superado algún límite de sus licencias y se ha utilizado entre un 100 % y un 110 % del total de unidades con licencia cubiertas por una sola licencia. Los dispositivos cliente se mantienen protegidos aun cuando ocurre este evento. Puede responder al evento de los siguientes modos: • Revise la lista de dispositivos administrados. Elimine los dispositivos que no estén en uso. • Agregue una licencia para más dispositivos (agregue un código de activación válido o un archivo de clave en el Servidor de administración).	90 días

			Kaspersky Security Center Cloud Console determina las reglas para generar eventos cuando se excede el límite de una licencia.	
El dispositivo ha permanecido inactivo en la red durante mucho tiempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Este tipo de evento ocurre cuando un dispositivo administrado se encuentra inactivo durante cierto tiempo. La mayoría de las veces, esto sucede porque el dispositivo se ha dado de baja. Puede responder al evento de los siguientes modos: • Elimine el dispositivo manualmente de la lista de dispositivos administrados. Especifique el intervalo de tiempo después del cual se crea el evento **El dispositivo ha permanecido inactivo en la red durante mucho tiempo.** El evento se crea con Kaspersky Security Center Cloud Console. • Especifique el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo con Kaspersky Security Center Cloud Console.	90 días
Conflicto de nombres de dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	Este tipo de evento ocurre cuando el Servidor de administración considera que dos o más dispositivos administrados son un mismo dispositivo. Aunque la clonación no es compatible con Kaspersky Security Center Cloud Console, este evento puede ocurrir si realiza la clonación utilizando una herramienta de terceros. Para evitar este evento, al copiar la imagen de un dispositivo con Agente de red instalado, debe seguir las siguientes recomendaciones: • En el dispositivo de referencia, detenga el servicio del Agente de red y ejecute la utilidad klmover con la clave -dupfix. 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 (requisito obligatorio) antes de la primera ejecución del servicio del Agente de red en dispositivos de destino, durante el primer inicio del sistema operativo después del despliegue de la imagen. La utilidad klmover viene incluida en el paquete de instalación del Agente de red. Si captura la imagen de un dispositivo que no tenga el Agente de red instalado, realice el despliegue de la imagen en los dispositivos de destino y luego implemente el Agente de red. Debe proporcionar acceso a la carpeta de red donde se encuentre los paquetes de instalación independientes desde un dispositivo.	90 días
El estado del dispositivo es Advertencia	4114	KLSRV_HOST_STATUS_WARNING	Este tipo de evento ocurre cuando se le asigna el estado *Advertencia* a un dispositivo administrado. Puede configurar las condiciones bajo las cuales el estado del dispositivo cambia a *Advertencia*.	90 días
Pronto se alcanzará el límite de instalaciones	4127	KLSRV_INVLICPROD_FILLED	Este tipo de evento ocurre cuando el número de instalaciones para las aplicaciones de terceros incluidas en un grupo de aplicaciones con licencia alcanza el 90 % del	90 días

de uno de los grupos de aplicaciones con licencia			valor máximo permitido en las propiedades de la clave de licencia. Puede responder al evento de los siguientes modos: • Si la aplicación de terceros no se utiliza en algunos de los dispositivos administrados, elimínela de esos dispositivos. • 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. 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	Este tipo de evento ocurre cuando un certificado de la característica Administración de dispositivos móviles no se vuelve a emitir automáticamente. Estas pueden ser las causas del evento y las respuestas adecuadas: • Se ha iniciado la nueva emisión automática de un certificado para el que la opción **Se ha solicitado el certificado** está desactivada. Esto puede deberse a un error ocurrido durante la creación del certificado. Es posible que se requiera la reemisión manual del certificado. • Si ha configurado la integración con una infraestructura de claves públicas, la causa podría ser la falta de un atributo SAM-Account-Name de la cuenta utilizada para la integración con dicha infraestructura y para la emisión del certificado. Revise las propiedades de la cuenta.	90 días
El certificado se ha eliminado	4134	KLSRV_CERTIFICATE_REMOVED	Este tipo de evento ocurre cuando un administrador elimina un certificado de cualquier tipo (general, de correo o de VPN) para Administración de dispositivos móviles. 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. Este evento puede resultar útil a la hora de investigar fallas asociadas con la administración de dispositivos móviles.	90 días
El certificado de APNs ha caducado	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Este tipo de evento ocurre cuando caduca un certificado de APNs. Debe renovar manualmente el certificado de APNs e instalarlo en un servidor de MDM para iOS.	90 días
El certificado de APNs caducará pronto	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Este tipo de evento ocurre cuando quedan menos de catorce días para que caduque el certificado de APNs. Cuando el certificado de APNs caduque, deberá renovarlo manualmente e instalarlo en un servidor de MDM para iOS. Le recomendamos que programe la renovación del certificado de APNs para antes de la fecha de caducidad.	90 días

No se ha podido enviar el mensaje FCM al dispositivo móvil	4138	KLSRV_GCM_DEVICE_ERROR	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. Lea el código HTTP en los detalles de la descripción del evento y responda en consecuencia. Para obtener más información sobre los códigos HTTP recibidos del servidor de FCM y los errores relacionados, consulte la documentación del servicio Google Firebase (en especial, el capítulo "Códigos de respuesta de errores de mensajes descendentes").	90 días
Se produjo un error de HTTP al enviar el mensaje FCM al servidor FCM	4139	KLSRV_GCM_HTTP_ERROR	Este tipo de evento ocurre cuando la característica Administración de dispositivos móviles está configurada para utilizar Google 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). Estas pueden ser las causas del evento y las respuestas adecuadas: • Problemas en el servidor de FCM. Lea el código HTTP en los detalles de la descripción del evento y responda en consecuencia. Para obtener más información sobre los códigos HTTP recibidos del servidor de FCM y los errores relacionados, consulte la documentación del servicio Google Firebase (en especial, el capítulo "Códigos de respuesta de errores de mensajes descendentes"). • Problemas en el servidor proxy (si usa un servidor proxy). Lea el código HTTP en los detalles del evento y actúe en consecuencia.	90 días
No se ha podido enviar el mensaje FCM al servidor FCM	4140	KLSRV_GCM_GENERAL_ERROR	Este tipo de evento ocurre cuando suceden errores inesperados del lado del Servidor de administración al utilizar el protocolo HTTP de Google Firebase Cloud Messaging. Lea los detalles en la descripción del evento y responda en consecuencia. Si no puede encontrar la solución a un problema por su cuenta, le recomendamos que se comunique con el servicio de soporte técnico de Kaspersky.	90 días
Se ha interrumpido la conexión con el Servidor de administración secundario	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Este tipo de evento ocurre cuando se interrumpe una conexión con el Servidor de administración secundario. Consulte el registro del sistema operativo en el dispositivo en el que esté instalado el Servidor de administración secundario y responda en consecuencia.	90 días
Se ha interrumpido la conexión con el Servidor de administración principal	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Este tipo de evento ocurre cuando se interrumpe una conexión con el Servidor de administración principal. Consulte el registro del sistema operativo en el dispositivo en el que esté instalado el Servidor de administración principal y responda en consecuencia.	90 días

Auditoría: la prueba de conexión al servidor SIEM produjo un error	5120	KLAUD_EV_SIEM_TEST_FAILED	Los eventos de este tipo ocurren cuando falla una prueba de conexión automática al servidor SIEM.	90 días

Eventos del Servidor de administración: nivel Información

La siguiente tabla muestra los eventos del Servidor de administración de Kaspersky Security Center Cloud Console 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	Descripción	Plazo de almacenamiento predeterminado
Se ha consumido más del 90 % de la clave de licencia	4097	KLSRV_EV_LICENSE_CHECK_90	Este tipo de evento ocurre cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en los dispositivos cliente están cerca de superar algún límite de licencia y cuando se utilizó más de un 90 % del total de unidades con licencia cubiertas por una sola licencia. Los dispositivos cliente están protegidos incluso cuando se supera un límite de licencia. Puede responder al evento de los siguientes modos: • Revise la lista de dispositivos administrados. Elimine los dispositivos que no estén en uso. • Agregue una licencia para más dispositivos (agregue un código de activación válido o un archivo de clave en el Servidor de administración). Kaspersky Security Center Cloud Console determina las reglas para generar eventos cuando se excede el límite de una licencia.	30 días
Se ha detectado un nuevo dispositivo	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	Este tipo de evento ocurre cuando se descubren nuevos dispositivos en red.	30 días
El dispositivo se ha movido automáticamente de acuerdo con una regla	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	Este tipo de evento ocurre cuando los dispositivos se asignaron a un grupo según las reglas de movimiento de dispositivos.	30 días
El dispositivo se ha eliminado del grupo: inactivo en la red durante mucho tiempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	Los eventos de este tipo ocurren cuando los dispositivos se eliminan automáticamente de un grupo por inactividad.	30 días
Pronto se superará el límite de instalaciones de	4128	KLSRV_INVLICPROD_EXPIRED_SOON	Este tipo de evento ocurre cuando el número de instalaciones para las	30 días

uno de los grupos de aplicaciones con licencia (ya se ha usado más del 95 %)			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. Puede responder al evento de los siguientes modos: • Si la aplicación de terceros no se utiliza en algunos de los dispositivos administrados, elimínela de esos dispositivos. • 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. Para administrar las claves de licencia de sus aplicaciones de terceros, puede utilizar la característica de grupos de aplicaciones con licencia.	
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	Los eventos de este tipo ocurren cuando el token de Firebase Cloud Messaging ha cambiado en el dispositivo. Para obtener información sobre la rotación del token de FCM, consulte la documentación del servicio Firebase.	30 días
Las actualizaciones se han copiado correctamente en la carpeta especificada	4122	KLSRV_UPD_REPL_OK	Los eventos de este tipo ocurren cuando la tarea **Descargar actualizaciones en el repositorio del Servidor de administración** termina de copiar archivos a una carpeta especificada.	30 días
Se ha establecido la conexión con el Servidor de administración secundario	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Consulte el siguiente tema para obtener más información Creación de una jerarquía de Servidores de administración: adición de un Servidor de administración secundario.	30 días
Se ha establecido la conexión con el Servidor de administración principal	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 días
Las bases de datos se han actualizado (En Kaspersky Security Center Cloud Console, este tipo de evento solo está disponible para un Servidor de administración secundario).	4144	KLSRV_UPD_BASES_UPDATED	Los eventos de este tipo ocurren cuando la tarea **Descargar actualizaciones en el repositorio del Servidor de administración** termina de actualizar las bases de datos.	30 días
El proxy de KSN se ha iniciado. La comprobación de disponibilidad de KSN se ha completado correctamente	7718	KSNPROXY_STARTED_CON_CHK_OK		30 días
El proxy de KSN se ha	7720	KSNPROXY_STOPPED		30 días

detenido				
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	Este evento responde a cambios ocurridos en los siguientes objetos: • Grupo de administración • Grupo de seguridad • Usuario • Paquete • Tarea • Directiva • Servidores • Servidor virtual	30 días
Auditoría: El estado del objeto ha cambiado	4150	KLAUD_EV_TASK_STATE_CHANGED	Este evento ocurre, por ejemplo, cuando una tarea no se completa debido a un error.	30 días
Auditoría: Parámetros de grupo modificados	4149	KLAUD_EV_ADMGROUP_CHANGED	Los eventos de este tipo ocurren cuando se ha editado un grupo de seguridad.	30 días
Auditoría: las claves de cifrado se han importado o exportado del Servidor de administración	5100	KLAUD_EV_DPEKEYSEXPORT		30 días
Auditoría: la prueba de conexión al servidor SIEM fue exitosa	5110	KLAUD_EV_SIEM_TEST_SUCCESS		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 Fallo operativo

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center que tienen el nivel de gravedad **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. 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 Fallo operativo

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Error al instalar la actualización	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Los eventos de este tipo ocurren si la actualización automática y los parches para los	30 días

			componentes de Kaspersky Security Center Cloud Console no tuvieron éxito. El evento no está vinculado a la actualización de las aplicaciones de Kaspersky administradas. Lea la descripción del evento. El evento puede tener su origen en un problema de Windows ocurrido en el Servidor de administración. Si la descripción menciona algún problema con la configuración de Windows, resuelva ese problema.	
Error al instalar la actualización de software de terceros	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Los eventos de este tipo ocurren si las funciones de la Administración de vulnerabilidades y parches y la Administración de dispositivos móviles están en el uso, y si la instalación de actualizaciones de software de terceros no tuvo éxito. Compruebe si el enlace al software desarrollado por este tercero es válido. Lea la descripción del evento.	30 días
Error al instalar las actualizaciones de Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Este tipo de evento ocurre cuando no se pueden instalar las actualizaciones de Windows. Configurar las actualizaciones de Windows en una directiva del Agente de red. Lea la descripción del evento. Busque el error en Microsoft Knowledge Base. Póngase en contacto con el servicio de soporte técnico de Microsoft si no puede resolver el problema por su cuenta.	30 días

Eventos del Agente de red: nivel Advertencia

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center Linux que tienen el nivel de gravedad **Advertencia**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Agente de red: nivel Advertencia

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se ha devuelto una advertencia durante la instalación de la actualización del módulo de software	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 días
La instalación de la actualización de software de terceros ha finalizado con una advertencia	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 días
Se ha pospuesto la instalación de la actualización de software de terceros	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 días
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 de Kaspersky Security Center Linux que tienen el nivel de gravedad **Información**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Agente de red: nivel Información

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
La actualización de módulos del software se ha instalado correctamente	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 días
Se ha iniciado la instalación de la actualización de módulos de software	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 días
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
La aplicación de terceros se ha instalado	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	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 dispositivo	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 días
El dispositivo se ha autorizado	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 días
Escritorio compartido de Windows: se ha leído el archivo	7712	KLUSRLOG_EV_FILE_READ	30 días
Escritorio compartido de Windows: se ha modificado el archivo	7713	KLUSRLOG_EV_FILE_MODIFIED	30 días
Escritorio compartido de Windows: se ha iniciado la aplicación	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 días
Escritorio compartido de Windows: iniciado	7715	KLUSRLOG_EV_WDS_BEGIN	30 días
Escritorio compartido de Windows: detenido	7716	KLUSRLOG_EV_WDS_END	30 días
La actualización de software de terceros se ha instalado correctamente	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 días
Se ha iniciado la instalación de la actualización de software de terceros	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 días
El proxy de KSN se ha iniciado. La 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 crear y ver selecciones de eventos definidos por el usuario según la configuración disponible en la interfaz de Kaspersky Security Center Cloud Console para configurarlas.

Las selecciones de eventos están disponibles en Kaspersky Security Center Cloud Console, en la sección **Control e informes**, al hacer clic en **Selecciones de eventos**.

De manera predeterminada, las selecciones de eventos incluyen información de los últimos siete días.

Kaspersky Security Center Cloud Console tiene un conjunto predeterminado de las selecciones (predefinidas) del evento:

- Eventos con distintos niveles de importancia:
  - **Eventos críticos**
  - **fallos operativos**
  - **Advertencias**
  - **Mensajes de información**
- **Solicitudes de usuario** (eventos de aplicaciones administradas)
- **Eventos recientes** (de la semana anterior)
- Eventos de auditoría

  En Kaspersky Security Center Cloud Console, se muestran los eventos de auditoría relacionados con las operaciones de servicio en su espacio de trabajo. Estos eventos están condicionados por las acciones de los especialistas en Kaspersky. Estos eventos, por ejemplo, incluyen lo siguiente: cambio de puertos del Servidor de administración; copia de seguridad de la base de datos del Servidor de administración; creación, modificación y eliminación de cuentas de usuario.

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 Cloud Console 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 Cloud Console 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 Cloud Console (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 Cloud Console 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

Kaspersky Security Center Cloud Console permite guardar eventos de una selección de eventos en un archivo TXT.

Para exportar eventos a un archivo:

1. Genere una selección de eventos.
2. Active la casilla de verificación ubicada junto al evento pertinente.

   También puede seleccionar varios eventos o la selección de eventos completa.
3. Haga clic en el botón **Exportar a archivo**.

El evento seleccionado se exporta a un archivo TXT.

Acceder al historial de un objeto desde un evento

Puede acceder al historial de revisiones de un objeto compatible con la administración de revisiones desde un evento relacionado con la creación o modificación de ese objeto.

Para acceder al historial de un objeto desde un evento:

1. Genere una selección de eventos.
2. 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.

Registro de información sobre eventos para tareas y directivas

Esta sección ofrece recomendaciones sobre cómo minimizar la cantidad de eventos para tareas y directivas almacenadas en la base de datos de Kaspersky Security Center Cloud Console. De forma predeterminada, cada 1000 dispositivos tienen 100 000 eventos. Si se excede este límite, los nuevos eventos sobrescriben los antiguos. Como resultado, los eventos críticos pueden desaparecer. Además, puede suceder el evento de advertencia del Servidor de administración denominado **Se ha superado el límite del número de eventos en la base de datos, los eventos se han eliminado**. En estos casos, le recomendamos que siga las instrucciones de esta sección.

Como resultado, aumentará la velocidad de ejecución de los escenarios asociados con el análisis de los eventos. Además, estas recomendaciones le ayudan a reducir el riesgo de que los eventos críticos se sobrescriban con una gran cantidad de eventos.

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 frecuencia (por ejemplo, más de una vez por semana), la cantidad 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, Kaspersky Security Center Cloud Console almacena solo información sobre el inicio, el progreso y la finalización (correcta, con una advertencia o un error) de la tarea de cada dispositivo en el que se ejecuta.

- **Guardar solo los resultados de ejecución de la tarea**. En este caso, Kaspersky Security Center Cloud Console almacena solo información sobre la finalización (correcta, con una advertencia o un error) de la tarea de cada dispositivo en el que se ejecuta.

Si se ha definido una directiva para un número bastante grande de dispositivos (por ejemplo, más de 10 000), la cantidad 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 activar su registro. Se recomienda desactivar el registro de todos los demás eventos.

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 de eventos si los eventos sobre cambios en los estados intermedios de las tareas de grupo y los eventos sobre la aplicación de directivas ocupan una gran parte de todos los eventos en la base de datos de Kaspersky Security Center Cloud Console.

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.

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.

Acerca de las notificaciones

Kaspersky Security Center Cloud Console ofrece la capacidad de supervisar la red de su organización enviando notificaciones sobre cualquier evento que considere importante. Se puede configurar notificaciones por correo electrónico para cualquier evento.

Al recibir notificaciones por correo electrónico, puede decidir su respuesta a un evento. Esta respuesta debe ser la más apropiada para la red de su organización.

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 por correo electrónico sobre eventos que ocurren en Kaspersky Security Center Cloud Console.

Para configurar la entrega de notificaciones de eventos que ocurren en Kaspersky Security Center Cloud Console:

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 configuración de las notificaciones de correo electrónico:

   Destinatarios (direcciones de correo electrónico)

Las direcciones de correo electrónico a las que Kaspersky Security Center Cloud Console enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma.

Puede especificar como máximo 24 direcciones de correo electrónico.

3. 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.

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 Cloud Console.

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.

Novedades de Kaspersky

En esta sección, encontrará información para utilizar, configurar y deshabilitar las novedades de Kaspersky.

Acerca de las novedades de Kaspersky

La sección Anuncios de Kaspersky (**Control e informes** → **Anuncios de Kaspersky**) le mantiene informado al brindarle información relacionada con Kaspersky Security Center Cloud Console y las aplicaciones administradas que están instaladas en los dispositivos administrados. Kaspersky Security Center Cloud Console actualiza periódicamente la información de la sección, eliminando anuncios desactualizados y añadiendo nueva información.

Kaspersky Security Center Cloud Console muestra solo los anuncios de Kaspersky que están 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.

Si hay varios administradores que usan Kaspersky Security Center Cloud Console y configuran diferentes idiomas de la interfaz, Kaspersky Security Center Cloud Console muestra los anuncios de Kaspersky en cada idioma utilizado por los administradores. Cuando cambia el idioma de la interfaz, los anuncios de Kaspersky en el idioma seleccionado se añaden a la sección automáticamente después de que cierra la sesión de la consola y vuelve a iniciar sesión.

Las novedades brindan información de distintas clases:

- Novedades sobre temas de seguridad

  Las novedades sobre seguridad están pensadas para que mantenga actualizadas y en perfectas condiciones de funcionamiento las aplicaciones de Kaspersky instaladas en su red. Estas novedades pueden dar aviso de actualizaciones críticas que se hayan publicado para las aplicaciones de Kaspersky, de soluciones disponibles para las vulnerabilidades detectadas o de formas de solucionar otros problemas en las aplicaciones de Kaspersky. Las novedades sobre seguridad están habilitadas de forma predeterminada. Si no desea recibir estas novedades, deshabilite la función correspondiente.

No puede desactivar los anuncios relacionados con la seguridad en el modo de prueba de Kaspersky Security Center Cloud Console.

Para mostrarle la información que corresponde a la configuración de la protección de su red, Kaspersky Security Center Cloud Console 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 Kaspersky Security Center Cloud Console que acepta cuando crea un espacio de trabajo para la empresa.

- 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 Cloud Console 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 información nueva en la sección Anuncios de Kaspersky, Kaspersky Security Center Cloud Console muestra una etiqueta de notificación que corresponde al nivel de importancia del anuncio. Haga clic en la etiqueta para ver la información en la sección de novedades 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 Cloud Console 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.

No puede desactivar los anuncios relacionados con la seguridad en el modo de prueba de Kaspersky Security Center Cloud Console.

Para dejar de recibir novedades sobre temas de seguridad:

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**, vaya a la sección **Anuncios de Kaspersky**.
3. Ponga el interruptor en la posición **Anuncios relacionados con la seguridad 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 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 **Configuración de KSN**.
3. Desactive la opción **Acepto usar Kaspersky Security Network**.
4. Haga clic en el botón **Guardar**.

   Ya no recibirá novedades con fines publicitarios.

Recepción de una advertencia de caducidad de la licencia

Para agregar clave de licencia de Kaspersky Endpoint Security for Business Select al Servidor de administración:

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**, seleccione la sección **Claves de licencia**.
3. Haga clic en **Seleccionar**.
4. En la ventana que se abre, seleccione la licencia y haga clic en **Aceptar**.

   De forma alternativa, si no se muestra ninguna licencia, puede hacer clic en **Añadir una nueva clave de licencia** y usar su código de activación.

La licencia se añadirá al repositorio del Servidor de administración. Esto hace que el Servidor de administración genere un evento crítico *La licencia caduca pronto* un día antes de que caduque el periodo de vigencia de la licencia y un evento crítico *Modo de funcionalidad limitada* después de que caduque el periodo de vigencia de la licencia. Si lo desea, puede configurar la entrega de notificaciones.

Si agrega clave de licencia de Kaspersky Endpoint Security for Business Select al repositorio del Servidor de administración, la licencia se considerará utilizada en un dispositivo.

Cloud Discovery

Kaspersky Security Center Cloud Console le permite supervisar el uso de servicios en la nube en dispositivos administrados con Windows y bloquear el acceso a los servicios en la nube que considere no deseados. Cloud Discovery rastrea los intentos del usuario de acceder a estos servicios mediante navegadores y aplicaciones de escritorio. Además, se rastrean los intentos del usuario de acceder a los servicios en la nube mediante conexiones no cifradas (por ejemplo, a través del protocolo HTTP). Con esta función podrá detectar y detener el uso de servicios en la nube que realice la TI invisible.

La función Cloud Discovery solo está disponible si ha comprado una licencia de Kaspersky Next. Para obtener información detallada, consulte el documento Licencias y la cantidad mínima de dispositivos para cada licencia.

Puede activar la función Cloud Discovery y elegir las directivas o los perfiles de seguridad para los que desea activar la función. También puede activar o desactivar la función en cada directiva o perfil de seguridad de forma independiente. Puede bloquear el acceso a los servicios en la nube a los que no desea que accedan los usuarios.

Para poder bloquear el acceso a servicios en la nube no deseados, asegúrese de que se cumplan los siguientes requisitos previos:

- Utiliza Kaspersky Endpoint Security 11.2 para Windows o una versión posterior. Las versiones anteriores de la aplicación de seguridad solo le permiten supervisar el uso de los servicios en la nube.
- Ha comprado una licencia de Kaspersky Next, que ofrece la posibilidad de bloquear el acceso a servicios en la nube no deseados. Para obtener más información, consulte la Ayuda de Kaspersky Next.

El widget de Cloud Discovery y los informes de Cloud Discovery muestran información sobre los intentos exitosos y bloqueados de acceder a servicios en la nube. El widget también muestra el nivel de riesgo de cada servicio en la nube. Kaspersky Security Center Cloud Console obtiene información sobre el uso de servicios de nube de todos los dispositivos administrados protegidos con directivas o los perfiles de seguridad que tengan la función activada.

Activar Cloud Discovery mediante el widget

La función Cloud Discovery le permite obtener información sobre el uso de los servicios en la nube de todos los dispositivos administrados que están protegidos solo con las directivas de seguridad que tienen la función activada. Puede activar o desactivar Cloud Discovery solo para la directiva de Kaspersky Endpoint Security para Windows.

Existen dos formas para activar la función Cloud Discovery:

- Mediante el widget de Cloud Discovery.
- En las propiedades de la directiva de Kaspersky Endpoint Security para Windows.

  Para obtener información detallada sobre cómo activar la función Cloud Discovery en las propiedades de la directiva de Kaspersky Endpoint Security para Windows, consulte la sección Cloud Discovery de la Ayuda de Kaspersky Endpoint Security para Windows.

Tenga en cuenta que solo puede desactivar la función Cloud Discovery en los parámetros de la directiva de Kaspersky Endpoint Security para Windows.

Para activar Cloud Discovery, debe tener el derecho de **Escribir** en el área funcional **Funciones generales: funcionalidad básica**.

Para activar la función Cloud Discovery mediante el widget:

1. Vaya a Kaspersky Security Center Cloud Console.
2. En el menú principal, vaya a **Control e informes** → **Panel**.
3. En el widget de **Cloud Discovery**, haga clic en el botón **Activar**.
4. En la ventana **Activar Cloud Discovery** que se abre, elija las directivas de seguridad para las que desea activar la función y, a continuación, haga clic en el botón **Activar**.

   Las siguientes configuraciones de directiva se activarán automáticamente: **Inyectar el script en el tráfico web para interactuar con las páginas web**, **Monitor de sesión web** y **Análisis de conexiones cifradas**.

La función Cloud Discovery se activa, y el widget se añade al panel.

Cómo añadir el widget de Cloud Discovery al panel

Puede añadir el widget de **Cloud Discovery** al panel para supervisar el uso de los servicios en la nube en los dispositivos administrados.

Para añadir el widget de Cloud Discovery al panel, debe tener el derecho de **Escribir** en el área **Funciones generales: funcionalidad básica**.

Para añadir el widget de Cloud Discovery al panel, haga lo siguiente:

1. Vaya a Kaspersky Security Center Cloud Console.
2. En el menú principal, vaya a **Control e informes** → **Panel**.
3. Haga clic en el botón **Añadir o restaurar un widget web**.
4. En la lista de widgets disponibles, haga clic en el icono de flecha (>) junto a la categoría **Otro**.
5. Elija el widget de **Cloud Discovery** y, luego, haga clic en el botón **Añadir**.

   Si la función Cloud Discovery está desactivada, siga las instrucciones en la sección Activar Cloud Discovery mediante el widget.

Los widgets elegidos se añaden al final del panel.

Visualizar información sobre el uso de servicios en la nube

Puede ver el widget de **Cloud Discovery** que muestra información sobre los intentos de acceso a los servicios en la nube. El widget también muestra el nivel de riesgo de cada servicio en la nube.
Kaspersky Security Center Cloud Console obtiene información sobre el uso de servicios de nube de todos los dispositivos administrados protegidos con directivas de seguridad que tengan la función activada.

Antes de la visualización, asegúrese de que:

- El widget de Cloud Discovery se haya añadido al panel.
- La función Cloud Discovery está activada.
- Tiene el derecho de **Leer** en el área funcional **Funciones generales: funcionalidad básica**.

Para ver el widget de Cloud Discovery:

1. Vaya a Kaspersky Security Center Cloud Console.
2. En el menú principal, vaya a **Control e informes** → **Panel**.

   El widget de **Cloud Discovery** aparecerá en el panel.
3. En el lateral izquierdo del widget de **Cloud Discovery**, elija una categoría de servicios en la nube.

   La tabla del lateral derecho del widget muestra hasta cinco servicios de la categoría elegida, a los que los usuarios intentan acceder con más frecuencia. Se consideran tanto los intentos exitosos como los bloqueados.
4. En el lateral derecho del widget, elija un servicio específico.

   La tabla a continuación muestra hasta diez dispositivos que intentan acceder al servicio con mayor frecuencia. En esta tabla, puede generar dos tipos de informes: informe sobre intentos de acceso exitosos e informe sobre intentos de acceso bloqueados.

   Además, en esta tabla puede bloquear el acceso al servicio de nube para un dispositivo específico.

El widget muestra la información solicitada.

Desde el widget mostrado, puede hacer lo siguiente:

- Continúe a la sección **Control e informes**→ **Informes** para ver los informes de Cloud Discovery.
- Bloquee o permita el acceso al servicio en la nube elegido.

La función Cloud Discovery solo está disponible si ha comprado una licencia de Kaspersky Next. Para obtener información detallada, consulte el documento Licencias y la cantidad mínima de dispositivos para cada licencia.

Nivel de riesgo de un servicio en la nube

Para cada servicio en la nube, Cloud Discovery le proporciona un nivel de riesgo. El nivel de riesgo le permite determinar los servicios que no se ajustan a los requisitos de seguridad de su organización. Por ejemplo, es posible que desee considerar el nivel de riesgo al decidir si bloquear el acceso a un determinado servicio.

El nivel de riesgo es un índice estimado y no dice nada acerca de la calidad de un servicio en la nube o acerca del fabricante del servicio. El nivel de riesgo es solo una recomendación de los expertos de Kaspersky.

Los niveles de riesgo de los servicios en la nube se muestran en el widget de Cloud Discovery y en la lista de todos los servicios en la nube supervisados.

Bloquear el acceso a servicios en la nube no deseados

Puede bloquear el acceso a los servicios en la nube a los que no desea que accedan los usuarios. También puede permitir el acceso a servicios en la nube que se habían bloqueado.

Entre otras consideraciones, es posible que desee considerar el nivel de riesgo al decidir si bloquear el acceso a un determinado servicio.

Puede bloquear o permitir el acceso a servicios en la nube para una directiva o perfil de seguridad.

Existen dos formas de bloquear el acceso a servicios en la nube no deseados:

- Mediante el widget de Cloud Discovery.

  En este caso, puede bloquear el acceso a los servicios uno a uno.

- En las propiedades de la directiva de Kaspersky Endpoint Security para Windows.

  En este caso, puede bloquear el acceso a los servicios uno a uno o bloquear una categoría completa.

  Para obtener información detallada sobre cómo activar la función Cloud Discovery en las propiedades de la directiva de Kaspersky Endpoint Security para Windows, consulte la sección Cloud Discovery de la Ayuda de Kaspersky Endpoint Security para Windows.

Para bloquear o permitir el acceso a un servicio en la nube mediante el widget:

1. Abra el widget de Cloud Discovery y elija el servicio en la nube que desee.
2. En el panel **Los principales 10 dispositivos que utilizan el servicio**, busque la directiva o el perfil de seguridad para el que desea bloquear o permitir el servicio.
3. En la línea requerida, en la columna **Estado del acceso en la directiva o el perfil**, realice una de las siguientes acciones:
   - Para bloquear el servicio, elija **Bloqueado** en la lista desplegable.
   - Para permitir el servicio, elija **Permitido** en la lista desplegable.
4. Haga clic en el botón **Guardar**.

El acceso al servicio elegido está bloqueado o permitido para la directiva o el perfil de seguridad.

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)** → **Grupos** → **<nombre del grupo>** → **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 pestaña **Avanzado**, 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 habilitar o deshabilitar el seguimiento.

   Se abre la lista de opciones de diagnóstico remoto.
4. Si desea habilitar el seguimiento, haga lo siguiente:

   a. En la sección **Seguimiento**, haga clic en **Activar seguimiento**.

   b. En la ventana **Modificar nivel de seguimiento**, recomendamos que mantenga los valores de configuración predeterminados. De ser necesario, un especialista del servicio de soporte técnico le indicará cómo modificar la configuración. Las opciones de configuración disponibles son las siguientes:

   - Nivel de seguimiento

     El nivel de seguimiento determina qué tan detallado es el archivo de seguimiento.

   - Seguimiento 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 Kaspersky Security Agent está regulado por la configuración del Agente de red. Por lo tanto, las opciones **Activar seguimiento** y **Modificar nivel de seguimiento** están desactivadas para este componente en los dispositivos cliente que ejecutan Linux.
5. Para deshabilitar el seguimiento para la aplicación seleccionada, haga clic en **Desactivar seguimiento**.

   Se deshabilita el seguimiento para la aplicación seleccionada.

Habilitar el seguimiento con Xperf

Si utiliza Kaspersky Endpoint Security, un especialista de nuestro servicio de soporte técnico podría pedirle que habilite el seguimiento con Xperf. Esta función permite obtener información sobre el rendimiento del sistema.

Para habilitar y configurar el seguimiento 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 **Seguimiento de Xperf**, haga clic en **Activar seguimiento de Xperf**.

   Si el seguimiento con Xperf ya está habilitado, verá, en cambio, el botón **Desactivar seguimiento 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 seguimiento de Xperf** en la sección **Seguimiento de Xperf**.

   Se deshabilita el seguimiento con Xperf.

Descargar los archivos de seguimiento de una aplicación

Puede descargar archivos de seguimiento desde un dispositivo cliente solo si se cumple una de las siguientes condiciones: la opción **No desconectar del Servidor de administración** está activada en la configuración del dispositivo, un servidor push está en uso o una puerta de enlace de conexión está en uso. De lo contrario, la descarga no es posible.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

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 **Seguimiento**, haga clic en el botón **Archivos de seguimiento**.

   Se abre la ventana **Registros de seguimiento del dispositivo**, en la que se muestra una lista de archivos de seguimiento.

5. En la lista de archivos de seguimiento, seleccione el archivo que desea descargar.

6. Realice una de las siguientes acciones:

   - Descargue el archivo seleccionado haciendo 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.

   Se abre la ventana **Registros de seguimiento del dispositivo**, en la que se muestra una lista de archivos de seguimiento.
4. En la lista de archivos de seguimiento, seleccione uno o varios archivos que desee eliminar.
5. Haga clic en el botón **Eliminar**.

Los archivos de seguimiento seleccionados quedan eliminados.

Descargar la configuración de las aplicaciones

Puede descargar la configuración de la aplicación desde un dispositivo cliente solo si se cumple una de las siguientes condiciones: la opción **No desconectar del Servidor de administración** está activada en la configuración del dispositivo, un servidor push está en uso o una puerta de enlace de conexión está en uso. De lo contrario, la descarga no es posible.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

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

Puede descargar información del sistema a su dispositivo desde un dispositivo cliente solo si se cumple una de las siguientes condiciones: la opción **No desconectar del Servidor de administración** está activada en la configuración del dispositivo, un servidor push está en uso o una conexión La puerta de enlace está en uso. De lo contrario, la descarga no es posible.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

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.

El archivo con la información se descarga en la ubicación especificada.

Descargar registros de eventos

Puede descargar registros de eventos a su dispositivo desde un dispositivo cliente solo si se cumple una de las siguientes condiciones: la opción **No desconectar del Servidor de administración** está activada en la configuración del dispositivo, un servidor push está en uso o una conexión La puerta de enlace está en uso. De lo contrario, la descarga no es posible.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

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.

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.

Realizar un diagnóstico remoto de una aplicación y descargar los resultados

Para realizar un diagnóstico de una aplicación instalada 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 la aplicación para la que desee realizar el diagnóstico remoto.

   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.

Si desea ejecutar un script personalizado en el dispositivo cliente, puede usar la variable de entorno `KLACDT_SAVE_SETTING` para determinar la ruta donde se guardarán los resultados de la ejecución. Por ejemplo:

- Para un dispositivo Windows:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```

- Para un dispositivo Linux:

  ```
  repetir algún resultado > $KLACDT_SAVE_SETTING/res.log
  ```

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 el campo **Tipo de objeto**, elija el tipo de objeto que desea cargar:
   - Elija **Archivo** para cargar el archivo ejecutable.
   - Elija **Carpeta** para cargar la carpeta que contiene la aplicación que desea ejecutar en el dispositivo cliente.

     Si elige este tipo de objeto, aparecerá el campo **Nombre del archivo ejecutable que debe ejecutarse**. En este campo, especifique el nombre del archivo ejecutable en la carpeta. También puede especificar la ruta relativa al archivo.
   - Elija **Archivo comprimido** para cargar el archivo comprimido ZIP que contiene la aplicación que desea ejecutar en el dispositivo cliente.

     Si elige este tipo de objeto, aparecerá el campo **Nombre del archivo ejecutable que debe ejecutarse**. En este campo, en la carpeta especifique el nombre del archivo ejecutable que desea ejecutar en el dispositivo cliente. También puede especificar la ruta relativa al archivo.

     El archivo ZIP debe incluir la carpeta de la utilidad. Esta carpeta contiene el archivo ejecutable que se ejecutará en un dispositivo remoto.
4. Cargue el objeto al elegirlo en la ventana del sistema o arrastrándolo al campo de carga.
5. Si es necesario, en el campo **Argumentos de la línea de comandos**, especifique los argumentos de la línea de comando que se pasarán al ejecutar el archivo ejecutable.
6. Haga clic en el botón **Cargar y ejecutar** para ejecutar la aplicación elegida en un dispositivo cliente.

7. Después de completar correctamente la ejecución de la aplicación, descargue los resultados de la ejecución haciendo clic en el botón **Descargar los resultados de la ejecución de la aplicación**.

   Los resultados de la ejecución de la aplicación se almacenan hasta que ejecute un nuevo diagnóstico o cierre la ventana.

Se completa el diagnóstico remoto del dispositivo cliente mediante la aplicación.

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 Cloud Console 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 Cloud Console, 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.

Exportación de eventos a sistemas SIEM

En esta sección, se brindan instrucciones para configurar la exportación de eventos a un sistema SIEM.

Configurar la exportación de eventos a sistemas SIEM

Esta sección proporciona un ejemplo de configuración de la exportación de eventos desde el Servidor de administración a sistemas SIEM externos. La exportación de la información acerca de eventos a sistemas SIEM externos permite a los administradores de sistemas SIEM responder lo antes posible a eventos del sistema de seguridad que ocurren en un dispositivo administrado o en grupos de dispositivos.

Requisitos previos

Antes de comenzar a configurar la exportación de eventos en Kaspersky Security Center Cloud Console:

- Lea sobre los métodos disponibles para exportar eventos.
- Asegúrese de conocer los valores de la configuración del sistema.

Los pasos aquí descritos pueden realizarse en cualquier orden.

Etapas

El proceso de exportación de eventos al sistema SIEM consta de las siguientes etapas:

- **Configuración del sistema SIEM para recibir eventos de Kaspersky Security Center Cloud Console**

  Debe configurar la recepción de eventos desde Kaspersky Security Center Cloud Console en el sistema SIEM.

- **Seleccione eventos para exportar**

  Debe seleccionar los eventos que desea exportar al sistema SIEM. En primer lugar, marque los eventos generales que ocurren en todas las aplicaciones administradas de Kaspersky. Además, puede marcar los eventos para determinadas aplicaciones administradas de Kaspersky.

- **Configuración de Kaspersky Security Center Cloud Console para exportar eventos al sistema SIEM**

  Debe configurar Kaspersky Security Center Cloud Console para iniciar la exportación de eventos al sistema SIEM.

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 Cloud Console, debe especificar ciertas configuraciones del sistema SIEM. Se recomienda que compruebe esta configuración de antemano a fin de prepararse para configurar Kaspersky Security Center Cloud Console.

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 la conexión entre Kaspersky Security Center Cloud Console y su servidor del sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center Cloud Console y en la configuración del receptor de su sistema SIEM.

- **Protocolo**

  Protocolo usado para transferir mensajes desde Kaspersky Security Center Cloud Console a su sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center Cloud Console y en la configuración del receptor de su sistema SIEM.

Acerca de la exportación de eventos

Kaspersky Security Center Cloud Console le permite recibir información sobre los eventos que ocurren durante el funcionamiento del Servidor de administración y las aplicaciones de Kaspersky instaladas en los 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 Cloud Console a sistemas SIEM externos involucra a dos partes: un remitente del evento – Kaspersky Security Center Cloud Console y un destinatario del evento – un sistema SIEM. Para exportar eventos correctamente, debe configurar estos parámetros en su sistema SIEM y en Kaspersky Security Center Cloud Console. No importa cuál de los dos lados se configura primero. Puede configurar la transmisión de eventos en Kaspersky Security Center Cloud Console y luego configurar su recepción por el 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 Cloud Console. 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.

Configuración de la exportación de eventos en un sistema SIEM

El proceso de exportar eventos desde Kaspersky Security Center Cloud Console a sistemas SIEM externos involucra a dos partes: un remitente del evento – Kaspersky Security Center Cloud Console y un destinatario del evento – un sistema SIEM. Debe configurar la exportación de eventos en su sistema SIEM y en Kaspersky Security Center Cloud Console.

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 Cloud Console, debe configurar el receptor en su sistema SIEM. Por lo general, deberá especificar los valores de los siguientes parámetros dentro del sistema SIEM:

- **Puerto**

  Especifique el número de puerto para conectar con Kaspersky Security Center Cloud Console. Este puerto debe ser igual que el puerto que especificó en Kaspersky Security Center Cloud Console durante la configuración con un sistema SIEM.

- **Protocolo de mensajes o tipo de origen**

  Especifique el formato Syslog.

Según el sistema SIEM utilizado, es posible que deba especificar la configuración del receptor adicional.

Analizadores sintácticos del mensaje

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 los mensajes son una parte del sistema SIEM; se utilizan para dividir los contenidos del mensaje en los campos relevantes, como ID del evento, gravedad, descripción, parámetros, etc. Esto permite al sistema SIEM procesar eventos recibidos de Kaspersky Security Center Cloud Console de modo que se puedan almacenar en la base de datos del sistema SIEM.

Marcar los eventos que se exportarán a un sistema SIEM en formato Syslog

Después de habilitar la exportación automática de eventos, debe seleccionar qué eventos se exportarán al sistema SIEM externo.

Para configurar la exportación de eventos en formato Syslog a un sistema externo, puede optar por una de estas vías:

- Marcar eventos generales. Si marca los eventos que desea exportar en la configuración de una directiva, en la configuración de los eventos o en la configuración del Servidor de administración, el sistema SIEM recibirá esos eventos cuando ocurran en cualquier aplicación sujeta a la directiva. Si los eventos exportados ya estaban seleccionados en la directiva, no podrá redefinirlos para una aplicación específica que esté administrada por esa directiva.

- Marcar eventos correspondientes a una aplicación administrada. Si marca eventos que correspondan a una aplicación administrada instalada en un dispositivo administrado, el sistema SIEM únicamente recibirá los eventos que ocurran en esa aplicación.

Marcar eventos de una aplicación de Kaspersky para 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). El estándar RFC 5424 se utiliza para exportar los eventos de Kaspersky Security Center Cloud Console a sistemas externos.

En Kaspersky Security Center Cloud Console, puede configurar la exportación de los eventos a los sistemas externos usando el protocolo de Syslog.

El proceso de exportación consta de dos pasos:

1. Habilitar la exportación de eventos automática. En este paso, Kaspersky Security Center Cloud Console se configura de modo que envíe eventos al sistema SIEM. Kaspersky Security Center Cloud Console empieza a enviar eventos inmediatamente después de que usted active 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 Cloud Console para exportar eventos al sistema SIEM

Para exportar eventos al sistema SIEM, debe configurar el proceso de exportación en Kaspersky Security Center Cloud Console.

Para configurar la exportación a sistemas SIEM en Kaspersky Security Center Cloud 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 la conexión entre Kaspersky Security Center Cloud Console y su servidor del sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center Cloud Console y en la configuración del receptor de su sistema SIEM.

- **Protocolo**

Puede utilizar solo el protocolo TLS sobre TCP para transferir mensajes al sistema SIEM. Para esto, especifique la configuración de TLS:

- **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 una cadena de certificados completa (incluido el certificado raíz) de una autoridad de certificados (CA) de confianza y cargar el archivo en Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console 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 SHA1 de la cadena de certificados completa del sistema SIEM (incluido el certificado raíz) en Kaspersky Security Center Cloud Console. Para añadir una huella digital SHA1, 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 Cloud Console. Por lo tanto, utilizará un certificado autofirmado emitido por Kaspersky Security Center Cloud Console. 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. Si el nombre de dominio del servidor del sistema SIEM no coincide con el nombre del sujeto del certificado del servidor del sistema SIEM, Kaspersky Security Center Cloud Console no podrá conectarse al 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 Cloud Console 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 Cloud Console.

  - **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 Cloud Console. Como resultado, Kaspersky Security Center Cloud Console 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. Para comprobar que la conexión del sistema SIEM esté configurada correctamente, haga clic en el botón **Comprobar conexión**.

   Se mostrará el estado de la conexión.

8. 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.

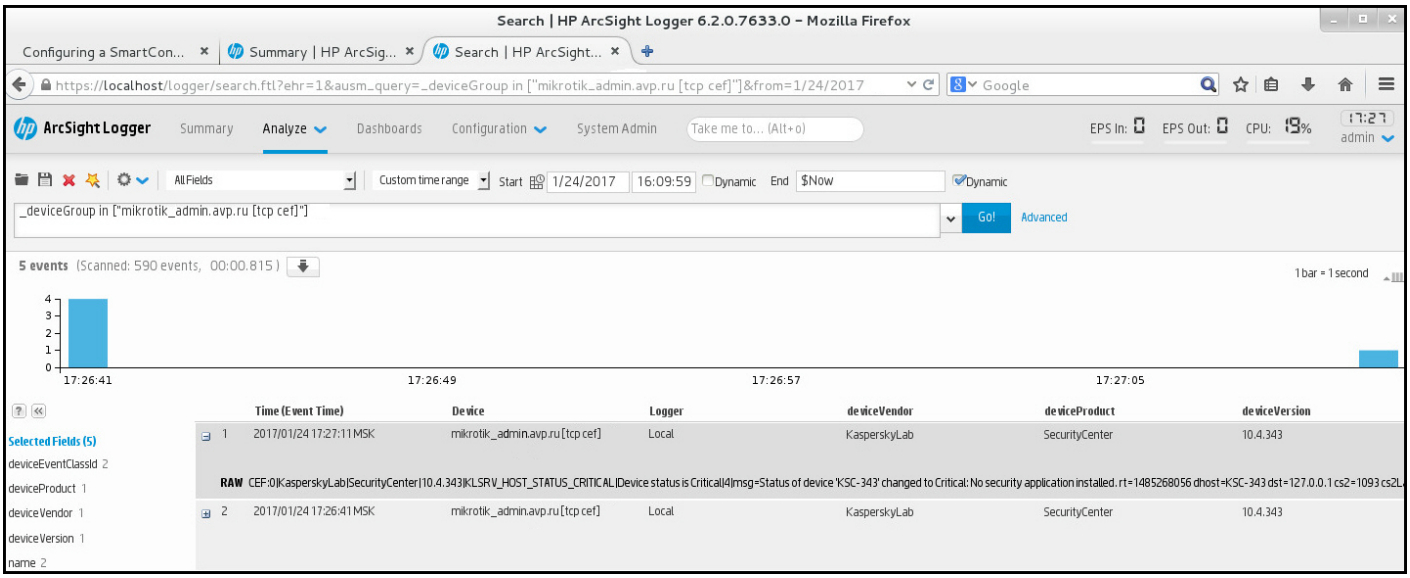
Ver los resultados de la exportación

Puede controlar si el procedimiento de exportación de eventos se ha completado debidamente. Para ello, verifique si el sistema SIEM recibe mensajes con los eventos exportados.

Si los eventos enviados desde Kaspersky Security Center Cloud Console se reciben y analizan correctamente por su sistema SIEM, la configuración en ambos lados se realiza correctamente. De otra forma, compruebe la configuración que especificó en Kaspersky Security Center Cloud Console con respecto a la configuración en su sistema SIEM.

La imagen de más abajo muestra los eventos exportados a ArcSight. El primero de ellos, *Device status is Critical*, es un evento crítico del Servidor de administración que se refiere al estado de un dispositivo.

La representación de los eventos exportados a un sistema SIEM varía según el sistema SIEM utilizado.



Ejemplo de eventos

Guía de inicio rápido para proveedores de servicios administrados (MSP)

Esta Guía de inicio rápido está destinada a administradores de proveedores de servicios gestionados (MSP).

Kaspersky Security Center Cloud Console admite el multiinquilinato. La guía contiene consejos y prácticas recomendadas para administrar las cuentas de sus clientes (inquilinos) e instalar aplicaciones de seguridad en sus dispositivos.

Acerca de Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console es una aplicación alojada y mantenida por Kaspersky. No es necesario instalar Kaspersky Security Center Cloud Console en su ordenador o servidor. Kaspersky Security Center Cloud Console permite al administrador instalar aplicaciones de seguridad de Kaspersky en dispositivos en una red corporativa, ejecutar tareas de análisis y actualización de forma remota y administrar las directivas de seguridad de las aplicaciones administradas. El administrador puede usar un panel de control detallado que proporciona una instantánea de los estados de los dispositivos corporativos, informes detallados y configuraciones granulares en las directivas de protección.

Características clave de Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console le permite hacer lo siguiente:

- Instalar aplicaciones de Kaspersky en dispositivos de su red y administrar aplicaciones instaladas.
- Crear una jerarquía de grupos de administración para administrar una selección de dispositivos cliente como si fueran una sola entidad.
- Crear Servidores de administración virtual y ordenarlos en una jerarquía.
- Proteger sus dispositivos de red, incluidas estaciones de trabajo y servidores:
  - Administre un sistema de protección antimalware creado según las aplicaciones Kaspersky.
  - Use las capacidades de detección y respuesta (EDR y MDR) (se requiere una licencia para Kaspersky Endpoint Detection and Response o para Kaspersky Managed Detection and Response), incluidas las siguientes:
    - Análisis e investigación de incidentes
    - Visualización de incidentes mediante la creación de un gráfico con la cadena de desarrollo de la amenaza
    - Aceptación o rechazo de respuestas de manera manual, o configuración de la aceptación automática de todas las respuestas
- Utilice Kaspersky Security Center Cloud Console como una aplicación de multiinquilinato.
- Gestione de forma remota las aplicaciones de Kaspersky instaladas en dispositivos cliente.
- Realizar un despliegue centralizado de claves de licencia para aplicaciones de Kaspersky en dispositivos cliente.
- Crear y administrar directivas de seguridad para dispositivos en su red.

- Crear y administrar cuentas de usuario.
- Cree y administre funciones de usuario (RBAC).
- Cree y administre tareas para las aplicaciones instaladas en sus dispositivos de red.
- Visualice informes sobre el estado del sistema de seguridad para cada organización cliente de manera individual.

Acerca de las licencias de Kaspersky Security Center Cloud Console para los MSP

Cuando comience a usar Kaspersky Security Center Cloud Console, puede solicitar un espacio de trabajo de prueba (en este caso, se le otorga una licencia de prueba de 30 días que está integrada a su espacio de trabajo) o introducir el código de activación de una licencia comercial.

No puede convertir un espacio de trabajo de prueba en uno comercial. Para continuar usando Kaspersky Security Center Cloud Console después de que caduque la licencia de prueba, debe eliminar el espacio de trabajo de prueba y crear otro con una licencia comercial.

Más tarde, puede añadir una o varias claves de licencia comerciales al repositorio del Servidor de administración.

Acerca de las capacidades de detección y respuesta para MSP

Kaspersky Security Center Cloud Console puede integrar funciones de otras aplicaciones de Kaspersky en la interfaz de la consola. Por ejemplo, puede añadir las funciones de detección y respuesta a la funcionalidad de Kaspersky Security Center Cloud Console mediante la integración de las siguientes aplicaciones:

- Kaspersky Endpoint Detection and Response Optimum

  Kaspersky Endpoint Detection and Response Optimum es una solución diseñada para proteger la infraestructura de TI de una organización de ciberamenazas complejas. La funcionalidad de la solución combina la detección automática de amenazas con la capacidad de responder a ellas para luchar contra ataques complejos, incluidos nuevos exploits, ransomware, ataques sin archivos y métodos que utilizan herramientas legítimas del sistema.

  Después de que una aplicación de Kaspersky Endpoint Protection Platform (EPP) detecte un incidente de seguridad, se genera una tarjeta detallada con información importante acerca del incidente de seguridad en Kaspersky Security Center Cloud Console. La tarjeta del incidente se genera a través de una de las siguientes aplicaciones:

  - Kaspersky Endpoint Agent que se instala junto con una aplicación de Kaspersky EPP
  - Kaspersky Endpoint Security para Windows 11.7.0 para Windows o versiones posteriores, que tiene una funcionalidad EDR Optimum integrada y no requiere de la instalación adicional de Kaspersky Endpoint Agent

  Una tarjeta de incidente le permite analizar e investigar el incidente. Además, puede visualizarlo mediante la creación de un gráfico con la cadena de desarrollo de la amenaza. El gráfico describe las etapas de despliegue del ataque detectado a tiempo. El gráfico creado incluye información acerca de los módulos involucrados en el ataque y las acciones llevadas a cabo por estos módulos.

También puede iniciar una cadena de acciones de respuesta: crear una regla de prevención de ejecución para un objeto que no es de confianza; buscar incidentes similares en el grupo de dispositivos, según los indicadores de compromiso (IOC) seleccionados; aislar un objeto que no es de confianza; aislar un dispositivo comprometido de la red.

Para obtener información sobre la activación de la aplicación, consulte la documentación de Kaspersky Endpoint Detection and Response Optimum.

Si se integra, esta aplicación añade la sección **Alertas** a la interfaz de Kaspersky Security Center Cloud Console (**Control e informes** → **Alertas**).

- Kaspersky Managed Detection and Response

  Kaspersky Managed Detection and Response brinda protección ininterrumpida contra el creciente volumen de amenazas que elude las barreras de seguridad automatizadas para las organizaciones que tienen dificultades para encontrar la experiencia y el personal adecuados o para aquellos que tienen recursos locales limitados. Los analistas de SOC (Centros de Operaciones de Seguridad) de MDR de Kaspersky o de una empresa externa investigan los incidentes y ofrecen respuestas para resolverlos. Puede aceptar o rechazar las medidas ofrecidas de forma manual o activar la opción para aceptar todas las respuestas automáticamente.

  Para obtener información sobre la activación de la aplicación, consulte la documentación de Kaspersky Managed Detection and Response.

  Si se integra, esta aplicación añade la sección **Incidentes** a la interfaz de Kaspersky Security Center Cloud Console (**Control e informes** → **Incidentes**).

Puede mostrar u ocultar los elementos de la interfaz que hacen referencia a las funciones de Kaspersky Endpoint Detection and Response o Kaspersky Managed Detection and Response en cualquier momento en la sección **Opciones de interfaz** de Kaspersky Security Center Cloud Console.

Guía de inicio rápido de Kaspersky Security Center Cloud Console

Después de completar las acciones enumeradas en esta sección, Kaspersky Security Center Cloud Console queda lista para usar.

Escenario de inicio

El escenario avanza en etapas:

1. **Crear una cuenta**

   Para comenzar a usar Kaspersky Security Center Cloud Console, necesita una cuenta.

   Para crear una cuenta:

   1. Abra su navegador e introduzca la siguiente dirección: https://ksc.kaspersky.com.
   2. Haga clic en el botón **Crear una cuenta**.
   3. Siga las instrucciones que se muestran en la pantalla.

2. **Crear un espacio de trabajo**

   Después de crear la cuenta, puede registrar su empresa y crear su espacio de trabajo.

   Cuando comience a usar Kaspersky Security Center Cloud Console, puede solicitar un espacio de trabajo de prueba (en este caso, se le otorga una licencia de prueba de 30 días que está integrada a su espacio de trabajo) o introducir el código de activación de una licencia comercial.

No puede convertir un espacio de trabajo de prueba en uno comercial. Para continuar usando Kaspersky Security Center Cloud Console después de que caduque la licencia de prueba, debe eliminar el espacio de trabajo de prueba y crear otro con una licencia comercial.

Para registrar una empresa y crear un espacio de trabajo

1. Abra su navegador e introduzca la siguiente dirección: https://ksc.kaspersky.com.
2. Haga clic en el botón **Iniciar sesión**.
3. Siga las instrucciones que aparezcan en pantalla.

3. **Realice la configuración inicial de Kaspersky Security Center Cloud Console**

   Cuando entre por primera vez al espacio de trabajo creado, se le solicitará automáticamente que ejecute el asistente de inicio rápido. El asistente de inicio rápido lo guía para crear un mínimo de tareas y directivas necesarias, ajustar un mínimo de configuraciones y comenzar a crear paquetes de instalación de las aplicaciones de Kaspersky. Siga las instrucciones que aparezcan en pantalla.

Una vez finalizada la configuración inicial, Kaspersky Security Center Cloud Console está lista para usar.

Recomendaciones sobre cómo administrar los dispositivos de sus clientes

Esta sección contiene recomendaciones para organizar los dispositivos de los clientes que desea proteger.

Las recomendaciones dependen de si está utilizando Kaspersky Security Center por primera vez o si ya ha utilizado la versión local:

- Si nunca ha usado Kaspersky Security Center, tiene dos opciones:
  - Crear un Servidor de administración virtual para los dispositivos de cada cliente (opción recomendada). En este caso, los dispositivos de cada cliente pueden administrarse a través de un Servidor de administración virtual dedicado e independiente de otros clientes. Al mismo tiempo, puede usar el Servidor de administración principal para crear políticas y tareas en común para todos los clientes. Los informes generados en el Servidor de administración principal pueden incluir datos de todos los Servidores de administración virtual.
  - Crear un grupo de administración para los dispositivos de cada cliente. Si desea dividir aún más los dispositivos de los clientes, puede crear una jerarquía de grupos de administración subordinados en cada grupo principal. Por ejemplo, es posible que necesite grupos subordinados si desea utilizar diferentes configuraciones de protección para los dispositivos de empleados que trabajan en diferentes departamentos.
- Si ya ha usado Kaspersky Security Center en las instalaciones, puede migrar sus grupos de administración y objetos relacionados existentes de Kaspersky Security Center en las instalaciones a Kaspersky Security Center Cloud Console.

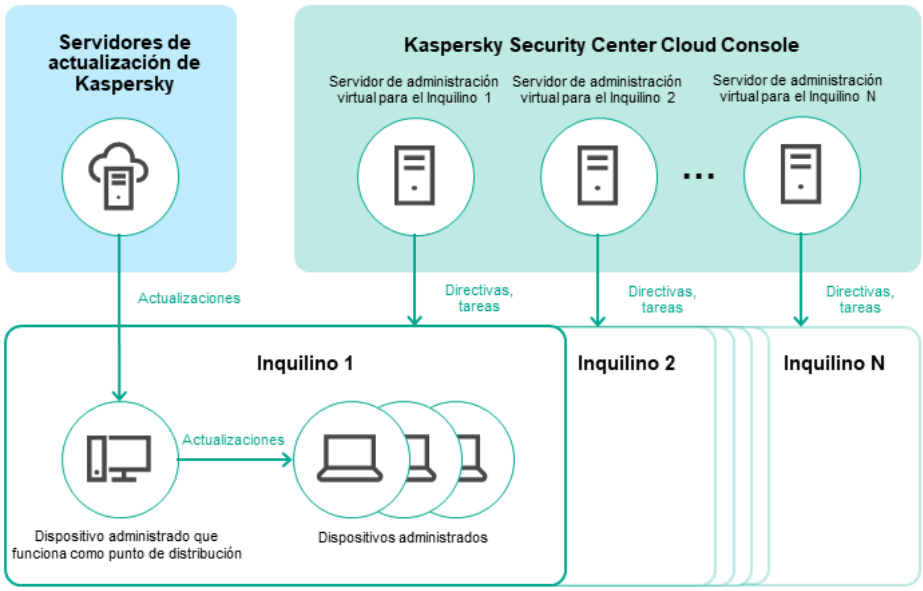
  No puede migrar los Servidores de administración virtual. Después de migrar los grupos de administración y otros objetos, puede crear Servidores de administración virtual en Kaspersky Security Center Cloud Console.

  Proceda a configurar la migración.

El administrador de un Servidor de administración virtual solo puede proceder a este Servidor virtual desde el Servidor de administración principal. El administrador de un Servidor de administración virtual tiene acceso de lectura a todos los objetos creados en el Servidor de administración principal (por ejemplo, widgets, informes o funciones de usuario).

Esquema de despliegue típico para MSP

En esta sección se proporciona una descripción del esquema de despliegue que los MSP utilizan típicamente para administrar varios inquilinos. El esquema se basa en la administración a través de Servidores de administración virtual creados de manera individual para cada inquilino.



Esquema de despliegue típico para MSP

El esquema abarca los siguientes componentes principales:

- *Kaspersky Security Center Cloud Console*. Proporciona una interfaz de usuario a los servicios de administración de su espacio de trabajo. Usted utiliza Kaspersky Security Center Cloud Console para desplegar, administrar y mantener el sistema de protección de la red de la organización cliente.
- *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 administración virtual*. Por lo general, un administrador de MSP crea un Servidor de administración virtual para que cada inquilino despliegue, administre y mantenga el sistema de protección de la red de la organización cliente correspondiente.
- *Inquilinos*. Las organizaciones cliente cuyos dispositivos deben protegerse.
- *Dispositivos administrados*. Dispositivos de la empresa cliente protegidos por Kaspersky Security Center Cloud Console. Cada dispositivo que debe protegerse debe tener instalado un Agente de red y una de las aplicaciones de seguridad de Kaspersky.
- *Dispositivo administrado que funciona como punto de distribución*. Equipo que tiene instalado el Agente de red y se utiliza para la distribución de actualizaciones, el sondeo de la red, la instalación remota de aplicaciones, la recopilación de información sobre equipos en un grupo de administración o dominio de difusión. El administrador selecciona los dispositivos apropiados y les asigna puntos de distribución de forma manual.

Escenario: Despliegue de la protección (administración de inquilinos a través de los Servidores de administración virtual)

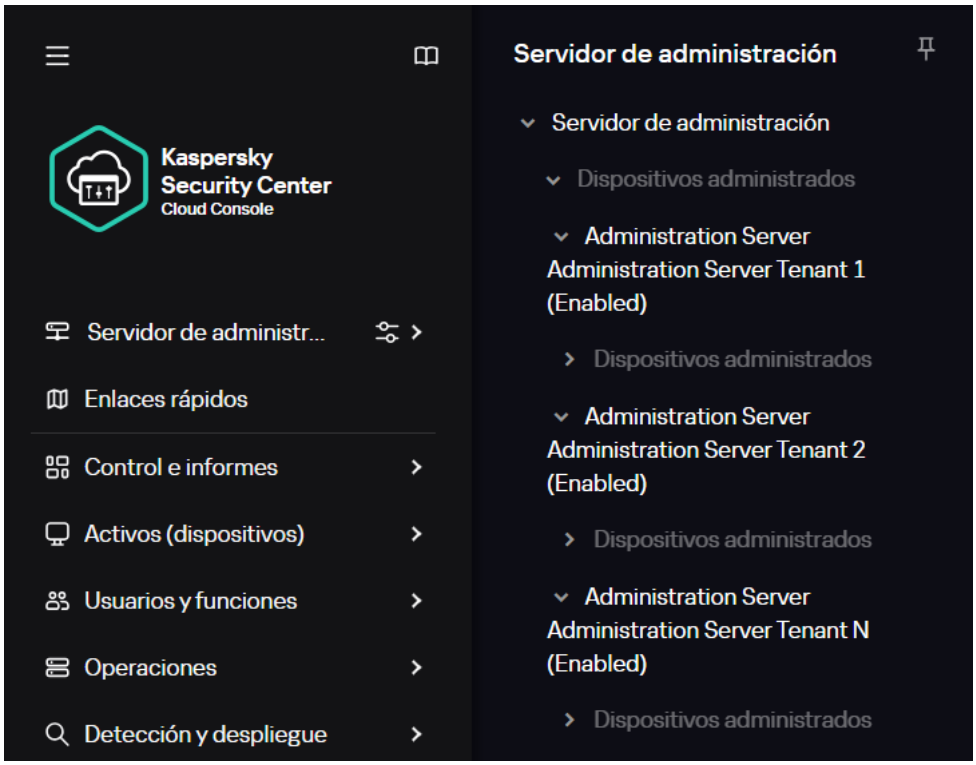
Si nunca ha usado Kaspersky Security Center y desea administrar sus inquilinos a través de Servidores de administración virtual, proceda como se describe en esta sección. Después de completar este escenario, los dispositivos de sus clientes estarán protegidos.

Si administra varios inquilinos, lleve a cabo el escenario para cada uno de ellos por separado.

El escenario avanza en etapas:

1. **Crear un Servidor de administración virtual**

   Cree un Servidor de administración virtual para su cliente. El nuevo Servidor de administración virtual aparece en la jerarquía de Servidores de administración:



   Servidores de administración virtual en la jerarquía de Servidores de administración

2. **Seleccionar un dispositivo para que actúe como un punto de distribución**

   Entre los dispositivos del cliente, decida qué dispositivo actuará como punto de distribución.

   > No puede tener más de 100 puntos de distribución dentro de un espacio de trabajo.

3. **Creación de un paquete de instalación independiente para el Agente de red**

   Cambie al Servidor de administración virtual creado y, luego, cree un paquete de instalación independiente del Agente de red. Para cambiar los Servidores de administración en el menú principal, haga clic en el icono de flecha (>) a la derecha del nombre del Servidor de administración actual y, luego, seleccione el Servidor de administración requerido. Durante la creación del paquete de instalación independiente, especifique el grupo de administración de dispositivos administrados al que desea mover el dispositivo.

4. **Instalación del Agente de red en el dispositivo seleccionado para que funcione como un punto de distribución**

   Puede usar cualquier método que le resulte adecuado:

   - Instalación manual

     Para entregar el paquete de instalación independiente al dispositivo, puede, por ejemplo, copiarlo en una unidad extraíble (como una unidad flash) o colocarlo en una carpeta compartida.

   - Despliegue mediante Active Directory.

   - Despliegue mediante el uso de su solución de software de supervisión y administración remota (RMM).

5. **Asignar un punto de distribución**

   Asigne el dispositivo con el Agente de red instalado para que funcione como punto de distribución.

6. **Sondeo de red**

   Configure y realice sondeos de red a través del punto de distribución.

   Kaspersky Security Center Cloud Console proporciona los siguientes métodos de sondeo de red:

   - Sondeo de intervalos IP

   - Sondeo de la red de Windows

   - Sondeo de Active Directory

   Después de completar el sondeo de red de acuerdo con el cronograma, los dispositivos de sus clientes se descubren y se colocan en el grupo **Dispositivos no asignados**.

7. **Mover los dispositivos descubiertos a los grupos de administración**

   Configure las reglas para mover automáticamente los dispositivos descubiertos a los grupos de administración requeridos; o bien mueva estos dispositivos manualmente a los grupos de administración requeridos. Si tiene pensado administrar los dispositivos del cliente en un único grupo de administración, puede mover los dispositivos al grupo de dispositivos administrados.

8. **Crear paquetes de instalación para el Agente de red y las aplicaciones administradas de Kaspersky**

   Cree paquetes de instalación para aplicaciones de Kaspersky.

9. **Eliminación de las aplicaciones de seguridad de terceros**

   Si hay aplicaciones de seguridad de terceros instaladas en los dispositivos de sus clientes, elimínelas antes de instalar las aplicaciones de Kaspersky.

10. **Instalación de aplicaciones de Kaspersky en dispositivos cliente**

    Cree tareas de instalación remota para instalar el Agente de red y las aplicaciones de Kaspersky administradas en los dispositivos de sus clientes.

    De ser necesario, también puede crear varias tareas de instalación remota para instalar las aplicaciones administradas de Kaspersky en diferentes grupos de administración o diferentes selecciones de dispositivos.

    Después de crear las tareas, puede configurarlas. Asegúrese de que la programación de cada tarea cumpla con sus requisitos. Primero, se debe ejecutar la tarea que instalará el Agente de red. Después de instalar el Agente de red en los dispositivos de sus clientes, se debe ejecutar la tarea que instalará las aplicaciones administradas de Kaspersky.

11. **Verificación del despliegue inicial de las aplicaciones de Kaspersky**

Genere y lea el **Informe de versiones de la aplicación de Kaspersky**. Asegúrese de que las aplicaciones administradas de Kaspersky estén instaladas en todos los dispositivos de su cliente.

12. **Crear directivas para las aplicaciones de Kaspersky**

    Cree una directiva para la aplicación de Kaspersky requerida. Si desea crear una directiva universal para todos los clientes, cambie el Servidor de administración virtual actual al Servidor de administración principal y, luego, cree una directiva para la aplicación de Kaspersky requerida.

Escenario: Despliegue de la protección (administración de inquilinos a través de los grupos de administración)

Si nunca ha usado Kaspersky Security Center y desea administrar sus inquilinos a través de grupos de administración, proceda como se describe en esta sección. Después de completar este escenario, los dispositivos de sus clientes estarán protegidos.

El escenario avanza en etapas:

1. **Creación de grupos de administración**

   Crear un grupo de administración para cada uno de sus clientes.

2. **Planificar la estructura de puntos de distribución**

   Entre los dispositivos de cada cliente, decida qué dispositivo actuará como punto de distribución.

   > No puede tener más de 100 puntos de distribución dentro de un espacio de trabajo.

3. **Creación de un paquete de instalación independiente para el Agente de red**

   Cree un paquete de instalación independiente para el Agente de red.

4. **Instalación del Agente de red en los dispositivos seleccionados para que funcionen como puntos de distribución**

   Instale el Agente de red en los dispositivos seleccionados que funcionarán como puntos de distribución.

   Puede usar cualquier método que le resulte adecuado:

   - Instalación manual

     Para entregar el paquete de instalación independiente a los dispositivos, puede, por ejemplo, copiarlo en una unidad extraíble (como una unidad flash) o colocarlo en una carpeta compartida.

   - Despliegue mediante Active Directory.

   - Despliegue mediante el uso de su solución de software de supervisión y administración remota (RMM).

5. **Designar los puntos de distribución**

   Asigne los dispositivos que tengan el Agente de red instalado para que funcionen como puntos de distribución.

6. **Sondeo de red**

   Configure y realice sondeos de red a través del punto de distribución.

   Kaspersky Security Center Cloud Console proporciona los siguientes métodos de sondeo de red:

- Sondeo de intervalos IP
- Sondeo de la red de Windows
- Sondeo de Active Directory

Después de completar el sondeo de red de acuerdo con el cronograma, los dispositivos de sus clientes se descubren y se colocan en el grupo **Dispositivos no asignados**.

7. **Mover los dispositivos descubiertos a los grupos de administración**

   Configure las reglas para mover automáticamente los dispositivos descubiertos a los grupos de administración requeridos; o bien mueva estos dispositivos manualmente a los grupos de administración requeridos.

8. **Crear paquetes de instalación para el Agente de red y las aplicaciones administradas de Kaspersky**

   Si no abrió el asistente de inicio rápido u omitió el paso de crear paquetes de instalación, cree paquetes de instalación para las aplicaciones de Kaspersky.

9. **Eliminación de las aplicaciones de seguridad de terceros**

   Si hay aplicaciones de seguridad de terceros instaladas en los dispositivos de sus clientes, elimínelas antes de instalar las aplicaciones de Kaspersky.

10. **Instalar aplicaciones de Kaspersky en los dispositivos de sus clientes**

    Cree tareas de instalación remota para instalar el Agente de red y las aplicaciones de Kaspersky administradas en los dispositivos de sus clientes.

    De ser necesario, también puede crear varias tareas de instalación remota para instalar las aplicaciones administradas de Kaspersky en diferentes grupos de administración o diferentes selecciones de dispositivos.

    Después de crear las tareas, puede configurarlas. Asegúrese de que la programación de cada tarea cumpla con sus requisitos. Primero, se debe ejecutar la tarea que instalará el Agente de red. Después de instalar el Agente de red en los dispositivos de sus clientes, se debe ejecutar la tarea que instalará las aplicaciones administradas de Kaspersky.

11. **Verificación del despliegue inicial de las aplicaciones de Kaspersky**

    Genere y lea el **Informe de versiones de la aplicación de Kaspersky**. Asegúrese de que las aplicaciones administradas de Kaspersky estén instaladas en todos los dispositivos de sus clientes.

12. **Crear directivas para las aplicaciones de Kaspersky**

    Diríjase al menú **Activos (dispositivos)** → **Grupos**. Si desea crear una directiva universal para todos sus clientes, seleccione **Servidor de administración.** Si desea crear una directiva específica para un cliente en particular, seleccione el grupo de administración de ese cliente. Cree una directiva para la aplicación de Kaspersky requerida.

Uso conjunto de Kaspersky Security Center y Kaspersky Security Center Cloud Console

Si ya ha utilizado Kaspersky Security Center Cloud Console localmente, puede convertir los Servidores de administración existentes que se ejecutan localmente en Servidores de administración secundarios de su nuevo Servidor de administración de Kaspersky Security Center Cloud Console, como se describe en esta sección.

Si configura el uso conjunto de Kaspersky Security Center (funcionando de forma local) y Kaspersky Security Center Cloud Console, no podrá migrar de la instancia local de Kaspersky Security Center a Kaspersky Security Center Cloud Console, a menos que elimine la jerarquía de Servidores de administración.

Para crear una jerarquía de Servidores de administración:

Añada los Servidores de administración existentes que se ejecutan localmente como Servidores de administración secundarios.

Licencias de aplicaciones de Kaspersky para los MSP

Kaspersky Security Center Cloud Console le permite realizar una distribución centralizada de las claves de licencia para las aplicaciones Kaspersky en los dispositivos de sus clientes, supervisar su uso y renovar las licencias.

Si administra varios inquilinos, puede distribuir claves de licencia de las siguientes maneras:

- Una clave de licencia para todos los inquilinos.
- Una clave de licencia individual para cada inquilino.

Para distribuir claves de licencia a los dispositivos de sus clientes:

1. Añada las claves de licencia requeridas al repositorio del Servidor de administración.
2. Realice una de las siguientes acciones:
   - Configure la distribución automática de una clave de licencia.

     En este caso, Kaspersky Security Center Cloud Console selecciona una de las claves de licencia aplicables y la instala automáticamente cada vez que se descubre un nuevo dispositivo.
   - Configure la tarea Añadir una clave para distribuir una clave de licencia a los dispositivos.

     Al configurar la tarea, seleccione la clave de licencia que debe implementarse en los dispositivos y seleccione el grupo de administración que contiene los dispositivos necesarios.

     Una tarea puede distribuir solo una clave de licencia. Significa que si desea distribuir varias claves de licencia, debe crear una tarea para cada una.

   Las aplicaciones de Kaspersky instaladas en los dispositivos de sus clientes ahora están activadas.

Es obligatorio añadir una clave de licencia activa al servidor de administración principal. De lo contrario, el espacio de trabajo asociado se eliminará en 90 días, independientemente del estado de las claves de licencia en otros servidores de administración dentro de ese espacio de trabajo.

Capacidades de supervisión e informes para los MSP

Kaspersky Security Center Cloud Console le brinda capacidades de supervisión y de creación de informes. Estas capacidades le brindan una descripción general de la infraestructura, estados de protección y estadísticas de su organización.

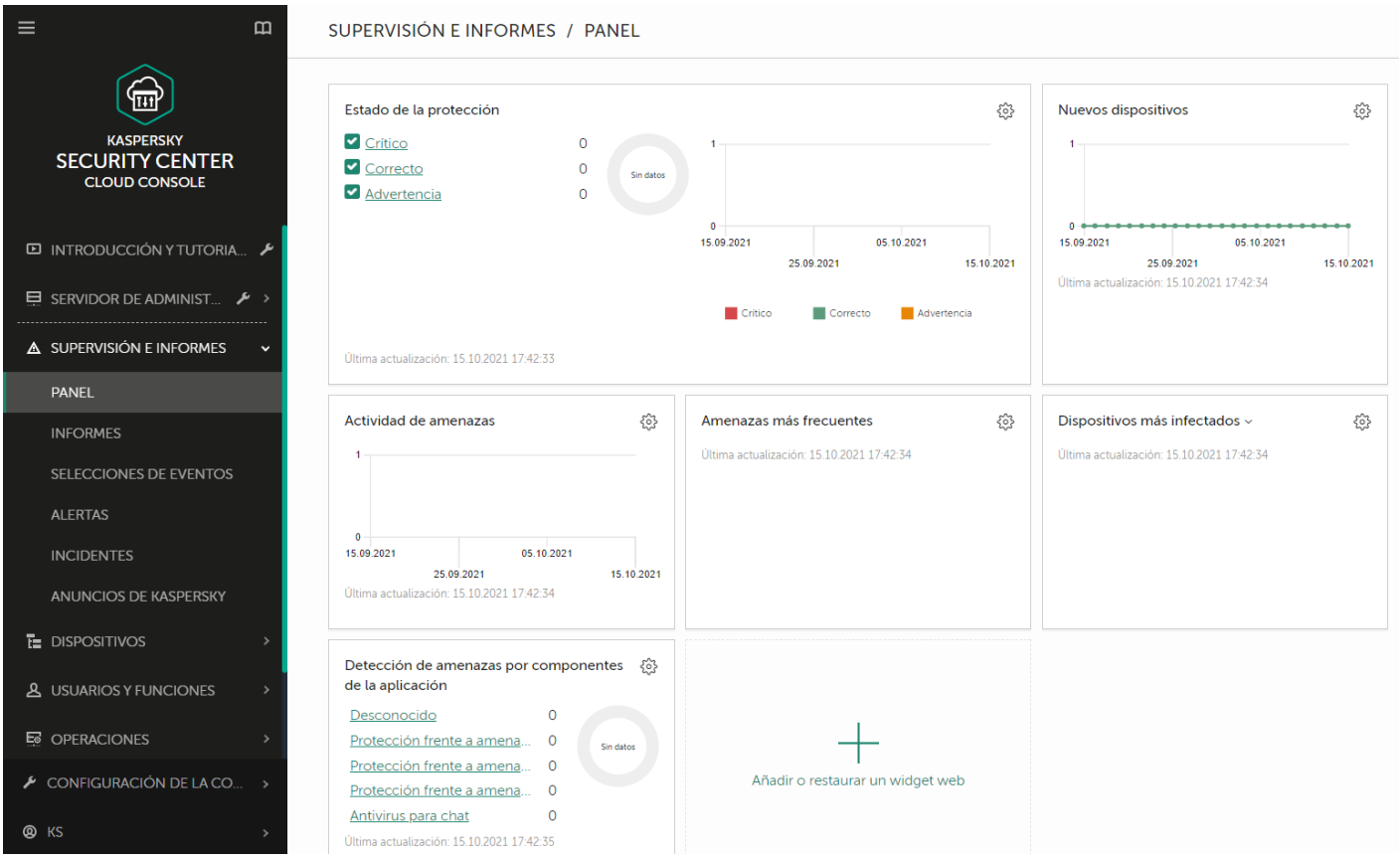
Una vez instalado Kaspersky Security Center Cloud Console, puede configurar las funciones de supervisión e informes para que se adapten mejor a sus necesidades.

Kaspersky Security Center Cloud Console proporciona los siguientes tipos de supervisión y de trabajo con informes:

- Panel
- Informes
- Selecciones de eventos
- Notificaciones por correo electrónico

Panel

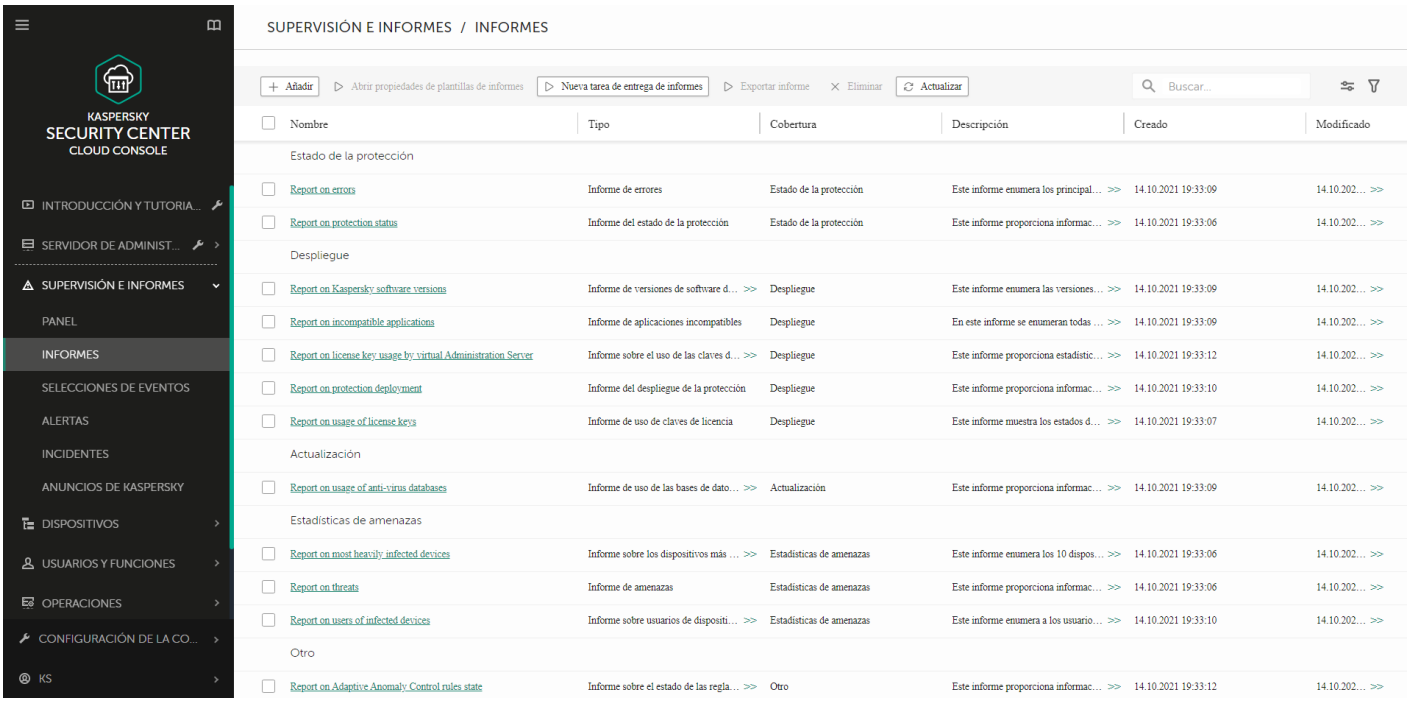
El panel brinda información gráfica que ayuda a controlar las tendencias de seguridad que se presentan en la red de la organización. (Vea la figura a continuación).



La sección del panel

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. También puede programar la entrega de informes por correo electrónico (consulte la figura a continuación).



La sección de informes

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. Kaspersky Security Center Cloud Console contiene varias selecciones de eventos predefinidas (por ejemplo, **Eventos recientes** y **Eventos críticos**) Además, puede crear selecciones personalizadas de eventos.

Notificaciones por correo electrónico

Puede configurar notificaciones por correo electrónico sobre eventos que ocurren en Kaspersky Security Center Cloud Console y en los dispositivos de sus clientes.

Trabajo con Kaspersky Security Center Cloud Console en un entorno de nube

Esta sección proporciona información sobre las características de Kaspersky Security Center Cloud Console relacionadas con la implementación y el mantenimiento de Kaspersky Security Center Cloud Console en entornos de nube, como Amazon Web Services, Microsoft Azure o Google Cloud.

Para trabajar en un entorno de nube, necesita una licencia especial. Si no dispone de dicha licencia, los elementos de la interfaz relacionados con los dispositivos en la nube no son operables.

Actualiza la funcionalidad (incluidas actualizaciones de firmas antivirus y actualizaciones de bases de código), además de la funcionalidad de KSN; puede no estar disponible en el software en los EE. UU.

Opciones de licencia en un entorno de nube

Trabajar en un entorno de nube es posible tanto en el modo de prueba, como en el modo comercial de Kaspersky Security Center Cloud Console:

- En el modo de prueba, todas las funciones del entorno de nube están disponibles durante todo el periodo de validez de su espacio de trabajo. No se requiere una licencia.
- En el modo comercial, las funciones del entorno de nube están disponibles solo si se ha añadido una clave de licencia de Kaspersky Hybrid Cloud Security como activa en las propiedades del Servidor de administración.

En ambos casos, Administración de vulnerabilidades y parches se activa automáticamente.

Si intenta activar la función "Soporte del entorno de nube" con la licencia de Kaspersky Hybrid Cloud Security, puede que se encuentre con un error.

Preparación para trabajar en un entorno de nube a través de Kaspersky Security Center Cloud Console

Esta sección le explica cómo es el trabajo de Kaspersky Security Center Cloud Console en los servicios web de Amazon.

- Amazon Web Services
- Microsoft Azure
- Google Cloud

Trabajar en el entorno de nube de Amazon Web Services

Esta sección le explica cómo prepararse para trabajar con Kaspersky Security Center Cloud Console en Amazon Web Services.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center Cloud Console.

Acerca del trabajo con el entorno de nube de Amazon Web Services

Para funcionar con la plataforma AWS y, en particular, para crear instancias, necesitará una cuenta de Amazon Web Services. Puede crear una cuenta sin costo en https://aws.amazon.com. Si ya tiene una cuenta de Amazon, puede usarla.

Encontrará información sobre las imágenes AMI y sobre el funcionamiento de la plataforma AWS en la página de ayuda de AWS Marketplace. Si precisa más información sobre el uso de la plataforma AWS, el uso de las instancias y otros conceptos, consulte la documentación de Amazon Web Services.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center Cloud Console.

Creación de cuentas de usuario de IAM para instancias de Amazon EC2

Esta sección describe las acciones que se deben realizar para garantizar el funcionamiento correcto de Kaspersky Security Center Cloud Console. Estas acciones incluyen el trabajo con las cuentas de usuario de AWS Identity and Access Management (IAM). También se describen las acciones que deberá realizar en los dispositivos cliente para instalar en ellos el Agente de red y, posteriormente, Kaspersky Security for Windows Server y Kaspersky Endpoint Security for Linux.

Asegurarse de que el Servidor de administración de Kaspersky Security Center Cloud Console tiene los permisos para funcionar con AWS

Para operar en el entorno de nube de Amazon Web Services utilizando Kaspersky Security Center Cloud Console, debe crear un *Cuenta de usuario de IAM*, que será utilizado por Kaspersky Security Center Cloud Console para trabajar con los servicios de AWS. Antes de comenzar a trabajar con el Servidor de administración, cree una cuenta de usuario de IAM con una *clave de acceso de AWS IAM* (en lo sucesivo, también se usará el término *clave de acceso de IAM*).

La creación de una cuenta de usuario de IAM requiere la Consola de administración de AWS. Para trabajar con la Consola de administración de AWS, necesitará el nombre de usuario y la contraseña de una cuenta de AWS.

Crear una cuenta de usuario de IAM para trabajar con Kaspersky Security Center Cloud Console

Se requiere una cuenta de usuario de IAM para trabajar con Kaspersky Security Center Cloud Console. Puede crear una cuenta de usuario de IAM con todos los permisos necesarios o, si lo prefiere, puede crear dos cuentas de usuario separadas.

Se crea automáticamente una *clave de acceso de IAM* para el usuario de IAM que deberá proporcionar a Kaspersky Security Center Cloud Console durante la configuración inicial. La clave de acceso de IAM consiste en un id. de clave de acceso y una clave secreta. Para obtener más información sobre el servicio de IAM, consulte las siguientes páginas de referencia de AWS:

- https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- https://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

Para crear una cuenta de usuario de IAM con los permisos necesarios, haga lo siguiente:

1. Abra la Consola de administración de AWS e inicie sesión con su cuenta.
2. En la lista de servicios AWS, seleccione **IAM**.

   Se abrirá una ventana con una lista de nombres de usuario y un menú para trabajar con la herramienta.
3. Navegue por las áreas de la consola relacionadas con las cuentas de usuario y agregue uno o más nombres de usuario nuevos.
4. Especifique las siguientes propiedades de AWS para cada usuario agregado:
   - Tipo de acceso: **Programmatic Access**.
   - Límite de permisos no establecido.
   - Permiso: **ReadOnlyAccess**.

     Después de añadir el permiso, compruebe que sea preciso. Si comete un error al hacer una selección, regrese a la pantalla anterior y vuelva a realizar la selección.
5. Después de crear la cuenta de usuario, aparecerá una tabla con la clave de acceso de IAM correspondiente al nuevo usuario de IAM. El id. de la clave de acceso estará en la columna **Access key ID**. La clave secreta se mostrará como una secuencia de asteriscos en la columna **Secret access key**. Para ver la clave secreta, haga clic en **Show**.

La cuenta que acaba de crear aparecerá en la lista de cuentas de usuario de IAM correspondiente a su cuenta de AWS.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center Cloud Console.

Trabajar en el entorno de nube de Microsoft Azure

Esta sección proporciona información sobre el despliegue de Kaspersky Security Center Cloud Console y el mantenimiento en un entorno de nube proporcionado por Microsoft Azure, así como detalles del despliegue de la protección en máquinas virtuales en este entorno de nube.

Acerca del uso de Microsoft Azure

Para trabajar con la plataforma Microsoft Azure y, en particular, para comprar aplicaciones en Azure Marketplace y crear máquinas virtuales, necesitará una suscripción de Azure. Antes de comenzar a trabajar con Microsoft Azure en Kaspersky Security Center Cloud Console, cree un ID de aplicación de Azure con los permisos necesarios para la instalación de aplicaciones en máquinas virtuales.

Creación de una suscripción, un id. de aplicación y una contraseña

Para trabajar con Kaspersky Security Center Cloud Console en el entorno de Microsoft Azure, necesita una suscripción de Azure, el id. de la aplicación de Azure y la contraseña de la aplicación Azure. Si ya tiene una suscripción, puede utilizarla.

Una suscripción de Azure otorga a su titular acceso al Portal de administración de la plataforma Microsoft Azure y a los servicios de Microsoft Azure. El titular puede usar la plataforma Microsoft Azure para administrar servicios como Azure SQL y Azure Storage.

Para crear una suscripción de Microsoft Azure,

Vaya a https://learn.microsoft.com/es-es/azure/cost-management-billing/manage/create-subscription y siga las instrucciones que allí se indican.

Encontrará más detalles sobre la creación de una suscripción en el sitio web de Microsoft website. Obtendrá una identificación de suscripción, que luego proporcionará a Kaspersky Security Center Cloud Console junto con el id. de la aplicación y la contraseña.

Para crear y guardar el id. de aplicación de Azure y su contraseña:

1. Vaya a https://portal.azure.com y constate que ha iniciado la sesión.
2. Siguiendo las instrucciones de la página de referencia, cree el id. de aplicación.
3. Vaya a la sección **Claves** de la configuración de la aplicación.
4. En la sección **Claves**, complete los campos **Descripción** y **Caducidad**, y deje el campo **Valor** en blanco.
5. Haga clic en **Guardar**.

   Cuando haga clic en **Guardar**, el sistema completará el campo **Valor** automáticamente con una larga secuencia de caracteres. Esta secuencia es la contraseña de la aplicación en Azure (por ejemplo, yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QIfFvdU=). La descripción se muestra a medida que la introduce.
6. Copie la contraseña y guárdela para que luego pueda proporcionar el id. y la contraseña de la aplicación a Kaspersky Security Center Cloud Console.

   Podrá copiar la contraseña solo en el momento en que se la cree. Más adelante, la contraseña ya no se mostrará y no podrá restaurarla.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center Cloud Console.

Asignación de una función al id. de la aplicación en Azure

Si solo desea detectar máquinas virtuales mediante el descubrimiento de dispositivos, el id. de la aplicación en Azure deberá tener la función de lector. Si no solo desea detectar máquinas virtuales, sino también implementar la protección mediante la API de Azure, su ID de aplicación de Azure debe tener la función de Virtual Machine Contributor.

Siga las instrucciones del sitio web de Microsoft para asignar una función al id. de la aplicación en Azure.

Trabajar con Google Cloud

Esta sección proporciona información sobre el trabajo con Kaspersky Security Center Cloud Console en un entorno de nube proporcionado por Google.

Puede usar la API de Google para trabajar con Kaspersky Security Center Cloud Console en Google Cloud Platform. Necesitará una cuenta de Google. Para más detalles, consulte la documentación publicada por Google en https://cloud.google.com.

Deberá crear las siguientes credenciales y proporcionárselas a Kaspersky Security Center Cloud Console:

- **Correo electrónico del cliente**

  La dirección de correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. de proyecto**

  El id. que le enviaron cuando registró su proyecto en Google Cloud.

- **Clave privada**

  La secuencia de caracteres que le enviaron como clave privada cuando registró su proyecto en Google Cloud. Recomendamos que copie y pegue esta secuencia para evitar errores.

Asistente de configuración del entorno de nube en Kaspersky Security Center Cloud Console

Para configurar Kaspersky Security Center Cloud Console usando este asistente, debe tener lo siguiente:

- Las credenciales específicas de un entorno de nube:
  - Un Cuenta de usuario de IAM a la que se le ha otorgado el derecho de sondear el segmento de la nube (para trabajar con Amazon Web Services)
  - Id. de aplicación, contraseña y suscripción de Azure (para operar con Microsoft Azure)
  - Correo electrónico del cliente, id. de proyecto y clave privada de Google (para operar con Google Cloud)
- Paquetes de instalación:
  - Agente de red para Windows

- Agente de red para Linux
- Kaspersky Endpoint Security for Linux

- Complemento web para Kaspersky Endpoint Security for Linux
- Al menos uno de los siguientes:
  - Paquete de instalación y complemento web para Kaspersky Endpoint Security para Windows (recomendado).
  - Paquete de instalación y complemento de administración de Kaspersky Security for Windows Server.

El Asistente de configuración del entorno de nube se inicia automáticamente durante la primera conexión a Kaspersky Security Center Cloud Console si su espacio de trabajo se creó con la licencia de Kaspersky Hybrid Cloud Security. También puede iniciar el Asistente de configuración del entorno de nube manualmente en cualquier momento.

Para iniciar el Asistente de configuración del entorno de nube manualmente,

En el menú principal, vaya a **Detección y despliegue → Despliegue y asignación → Configurar el entorno de nube**.

Se inicia el asistente.

La sesión de trabajo promedio con este asistente es aproximadamente 15 minutos.

Paso 1. Comprobar los complementos y paquetes de instalación necesarios

Este paso no se muestra si tiene todos los complementos web y paquetes de instalación necesarios que se enumeran a continuación.

Para configurar un entorno de nube, debe tener los siguientes componentes:

- Paquetes de instalación:
  - Agente de red para Windows
  - Agente de red para Linux
  - Kaspersky Endpoint Security for Linux
- Complemento web para Kaspersky Endpoint Security for Linux
- Al menos uno de los siguientes:
  - Paquete de instalación y complemento web para Kaspersky Endpoint Security para Windows (recomendado).
  - Paquete de instalación y complemento de administración de Kaspersky Security for Windows Server.

Le recomendamos que utilice Kaspersky Endpoint Security para Windows en lugar de Kaspersky Security for Windows Server.

Kaspersky Security Center Cloud Console detecta automáticamente los componentes que ya tiene y enumera solo los que faltan. Para descargar los componentes enumerados, haga clic en el botón **Seleccionar aplicaciones para descargar** y luego seleccione los complementos y paquetes de instalación requeridos. Después de descargar un componente, puede utilizar el botón **Actualizar** para actualizar la lista de componentes que faltan.

Paso 2. Selección del método de activación de la aplicación

Este paso se muestra solo si utilizó una licencia que no es de Kaspersky Hybrid Cloud Security durante la creación del espacio de trabajo y nunca agregó una clave de licencia de Kaspersky Hybrid Cloud Security al campo de activación del Servidor de administración. En este caso, debe activar el Servidor de administración con una licencia de Kaspersky Hybrid Cloud Security.

Paso 3. Selección del entorno de nube y autorización

Configure los siguientes ajustes:

- **Entorno de nube**

  Seleccione el entorno de nube en el que está desplegando Kaspersky Security Center Cloud Console: AWS, Azure o Google Cloud.

  Si planea trabajar con más de un entorno de nube, seleccione un entorno y luego ejecute el asistente de nuevo.

- **Nombre de la conexión**

  Escriba un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres Unicode.

  El nombre que escriba aquí será también el nombre del grupo de administración para los dispositivos de nube.

  Si planea trabajar con más de un entorno de nube, sugerimos que incluya el nombre del entorno en el nombre de la conexión (por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google").

Introduzca las credenciales para autorizarse en el entorno de nube seleccionado.

AWS

Si seleccionó AWS como el tipo de segmento de la nube, utilice una Clave de acceso de AWS IAM para seguir encuestando el segmento de la nube. Ingrese los siguientes datos clave:

- **Id. de la clave de acceso**

El id. de la clave de acceso de IAM es una secuencia de caracteres alfanuméricos. Obtuvo este id. al crear la cuenta de usuario de IAM.

El campo está disponible después de seleccionar una clave de acceso de AWS IAM para la autorización.

- **Clave secreta**

  La clave secreta que recibió con el id. de la clave de acceso al crear la cuenta de usuario de IAM.

  Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a escribir la clave secreta, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado el tiempo que necesite para ver los caracteres introducidos.

  El campo está disponible después de seleccionar una clave de acceso de AWS IAM para la autorización.

  Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

Azure

Si ha seleccionado Azure como tipo de segmento de nube, debe introducir los siguientes datos para permitir el sondeo del segmento:

- **Id. de la aplicación en Azure**

  Usted creó el id. de la aplicación en el portal de Azure.

  No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

- **Id. de suscripción de Azure**

  Creó esta suscripción en el portal de Azure.

- **Contraseña de la aplicación Azure**

  Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

  Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

  Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

- **Nombre de la cuenta de almacenamiento de Azure**

  Creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center Cloud Console.

- **Clave de acceso al almacenamiento de Azure**

Recibió una contraseña (clave) cuando creó la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center Cloud Console.

La clave está disponible en la sección "Descripción general de la cuenta de almacenamiento de Azure", en la subsección "claves".

Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

Google Cloud

Si ha seleccionado Google Cloud como tipo de segmento de nube, debe introducir los siguientes datos para permitir el sondeo del segmento:

- **Correo electrónico del cliente**

  La dirección de correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. del proyecto**

  El id. que le enviaron cuando registró su proyecto en Google Cloud.

- **Clave privada**

  La secuencia de caracteres que le enviaron como clave privada cuando registró su proyecto en Google Cloud. Recomendamos que copie y pegue esta secuencia para evitar errores.

  Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

La aplicación guarda la conexión configurada.

El Asistente de configuración del entorno de nube le permite especificar solo un segmento. Si necesita administrar otros segmentos de nube, podrá agregar las conexiones necesarias en otro momento.

Haga clic en **Siguiente** para continuar.

Paso 4. Sondeo de segmentos y configuración de la sincronización con la nube

En este paso, se inicia al sondeo de segmentos de la nube y se crea el grupo de administración especial para dispositivos de nube. Los dispositivos que se detecten durante el sondeo se agregarán a este nuevo grupo. El programa de sondeo de segmentos de la nube está configurado cada cinco minutos de forma predeterminada; (puede cambiar esta configuración más adelante).

La aplicación también creará una regla de movimiento automático llamada **Sincronizar con la nube**. Para cada análisis posterior de la red en la nube, los dispositivos virtuales que se detecten se moverán al subgrupo correspondiente dentro del grupo **Dispositivos administrados\Cloud**.

Definir la configuración **Sincronizar grupos de administración con estructura de nube**.

Si habilita está opción, se creará el grupo **Cloud** automáticamente dentro el grupo **Dispositivos administrados** y se iniciará un proceso para descubrir dispositivos en la nube. Las instancias y las máquinas virtuales que se detecten cada vez que se sondee la red de la nube se agregarán al grupo "Cloud". La estructura de subgrupos de administración dentro de este grupo se hará coincidir con la estructura del segmento de la nube (en AWS, las zonas de disponibilidad y los grupos de ubicación no estarán representados en la estructura; en Azure, no estarán representadas las subredes). Los dispositivos que no se hayan identificado como instancias en el entorno de nube estarán en el grupo **Dispositivos no asignados**. Esta estructura de grupo le permite usar tareas de instalación en grupo para instalar aplicaciones antivirus en instancias, así como configurar diferentes directivas para diferentes grupos.

Si no habilita esta opción, también se creará el grupo **Cloud** y también se iniciará el descubrimiento de dispositivos de la nube, pero no se crearán subgrupos que coincidan con la estructura del segmento de la nube dentro del grupo. Todas las instancias detectadas se agregarán al grupo de administración **Cloud** y aparecerán en una misma lista. Si su trabajo con Kaspersky Security Center Cloud Console requiere sincronización, puede modificar las propiedades de la regla **Sincronizar con Cloud** y aplicarla. Al aplicar la regla, la estructura de subgrupos del grupo "Cloud" se hará coincidir con la estructura del segmento de la nube.

Esta opción está deshabilitada de manera predeterminada.

Haga clic en **Siguiente** para continuar.

Paso 5. Seleccionar una aplicación para crear una directiva y tareas para

Este paso solo se muestra si tiene paquetes de instalación y complementos para Kaspersky Endpoint Security para Windows y Kaspersky Security for Windows Server. Si tiene un complemento y un paquete de instalación para solo una de esas aplicaciones, este paso se omite y Kaspersky Security Center Cloud Console crea una directiva y tareas para la aplicación existente.

Seleccione una aplicación para la que desea crear una directiva.

- Kaspersky Endpoint Security para Windows
- Kaspersky Security for Windows Server

Paso 6. Configuración de Kaspersky Security Network para Kaspersky Security Center Cloud Console

Este paso se omite cuando se ejecuta Kaspersky Security Center Cloud Console en modo de prueba o en un Servidor de administración virtual.

Especifique la configuración para transmitir la información sobre las operaciones de Kaspersky Security Center Cloud Console a la base de conocimientos de Kaspersky Security Network (KSN). Seleccione una de las siguientes opciones:

- **Acepto usar Kaspersky Security Network**

Kaspersky Security Center Cloud Console 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 Cloud Console y las aplicaciones administradas no proporcionarán información a Kaspersky Security Network.

  Si selecciona esta opción, se deshabilitará el uso de Kaspersky Security Network.

Kaspersky recomienda participar en Kaspersky Security Network.

Es posible que se le muestren los acuerdos de KSN correspondientes a las aplicaciones administradas. Si acepta usar Kaspersky Security Network, las aplicaciones administradas remitirán información a Kaspersky. Si no acepta participar en Kaspersky Security Network, la aplicación administrada no enviará datos a Kaspersky. Puede cambiar esta configuración más adelante en la directiva de la aplicación.

Haga clic en **Siguiente** para continuar.

Paso 7. Creación de una configuración de protección inicial

Puede ver la lista de directivas y tareas creadas.

Espere a que finalice la creación de las tareas y directivas. A continuación, haga clic en **Siguiente**. En la última página del asistente, haga clic en el botón **Finalizar** para salir.

Sondeo de segmentos de red a través de Kaspersky Security Center Cloud Console

La información sobre la estructura de la red (y los dispositivos en ella) se recibe a través del sondeo regular de los segmentos de la nube mediante las herramientas AWS API, Azure API o Google API. Kaspersky Security Center Cloud Console utiliza esta información para actualizar el contenido de las carpetas Dispositivos no asignados y Dispositivos administrados. Si se han configurado reglas de movimiento automático, los dispositivos detectados se agregan a los grupos de administración que les corresponden automáticamente.

Para permitir el sondeo de segmentos de la nube, debe tener los derechos correspondientes que se proporcionan con una cuenta de usuario de IAM (en AWS), o con ID de aplicación y contraseña (en Azure) o con un correo electrónico de cliente de Google, ID de proyecto de Google y clave privada (en Google Cloud).

Puede agregar y eliminar conexiones para cada segmento de nube y definir una programación de sondeo para cada segmento.

Añadir conexiones para el sondeo de segmentos de la nube a través de Kaspersky Security Center Cloud Console

Para agregar una conexión para sondear un segmento de nube a la lista de conexiones disponibles:

1. En el menú principal, vaya a **Detección y despliegue** → **Detección** → **Cloud**.
2. En la ventana que se abre, haga clic en **Propiedades**.
3. En la ventana **Configuración** que se abre, haga clic en **Añadir**.

   Se abre la ventana **Configuración de segmentos de la nube**.
4. Escriba el nombre del entorno de nube correspondiente a la conexión que se usará para sondear el segmento de nube:

   - **Entorno de nube**

     Seleccione el entorno de nube en el que está desplegando Kaspersky Security Center Cloud Console: AWS, Azure o Google Cloud.

     Si planea trabajar con más de un entorno de nube, seleccione un entorno y luego ejecute el asistente de nuevo.

   - **Nombre de la conexión**

     Escriba un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres Unicode.

     El nombre que escriba aquí será también el nombre del grupo de administración para los dispositivos de nube.

     Si planea trabajar con más de un entorno de nube, sugerimos que incluya el nombre del entorno en el nombre de la conexión (por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google").
5. Introduzca las credenciales para autorizarse en el entorno de nube seleccionado.

   - Si seleccionó AWS, especifique lo siguiente:

     - **Id. de la clave de acceso**

       El id. de la clave de acceso de IAM es una secuencia de caracteres alfanuméricos. Obtuvo este id. al crear la cuenta de usuario de IAM.

       El campo está disponible después de seleccionar una clave de acceso de AWS IAM para la autorización.

     - **Clave secreta**

       La clave secreta que recibió con el id. de la clave de acceso al crear la cuenta de usuario de IAM.

       Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a escribir la clave secreta, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado el tiempo que necesite para ver los caracteres introducidos.

       El campo está disponible después de seleccionar una clave de acceso de AWS IAM para la autorización.

     Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

- Si seleccionó Azure, configure los siguientes parámetros:
  - **ID de aplicación en Azure**

    Usted creó el id. de la aplicación en el portal de Azure.

    No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

  - **Id. de suscripción de Azure**

    Creó esta suscripción en el portal de Azure.

  - **Contraseña de la aplicación Azure**

    Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

    Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

    Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

  - **Nombre de la cuenta de almacenamiento de Azure**

    Creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center Cloud Console.

  - **Clave de acceso al almacenamiento de Azure**

    Recibió una contraseña (clave) cuando creó la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center Cloud Console.

    La clave está disponible en la sección "Descripción general de la cuenta de almacenamiento de Azure", en la subsección "claves".

    Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

Si seleccionó Google Cloud, configure los siguientes ajustes:

- **Correo electrónico del cliente**

  La dirección de correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. del proyecto**

  El id. que le enviaron cuando registró su proyecto en Google Cloud.

- **Clave privada**

La secuencia de caracteres que le enviaron como clave privada cuando registró su proyecto en Google Cloud. Recomendamos que copie y pegue esta secuencia para evitar errores.

Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

6. Si lo desea, haga clic en **Programar sondeo** y cambie la configuración predeterminada.

La conexión se guarda en la configuración de la aplicación.

Después de sondear el nuevo segmento de la nube por primera vez, el subgrupo correspondiente a ese segmento aparece en el grupo **Dispositivos administrados\Administración de la nube**.

Si las credenciales que introdujo no son correctas, no se encontrará ninguna instancia durante el sondeo del segmento y, en consecuencia, no aparecerá ningún subgrupo nuevo en el grupo de administración **Dispositivos administrados\Cloud**.

Eliminar conexiones para el sondeo de segmentos de nube

Si ya no necesita que la aplicación sondee un segmento de nube en particular, puede eliminar la conexión correspondiente a ese segmento de la lista de conexiones disponibles. Lo mismo puede hacer si, por ejemplo, los permisos para sondear el segmento se han transferido a un usuario que utiliza otras credenciales.

Para eliminar una conexión:

1. En el menú principal, vaya a **Detección y despliegue** → **Detección** → **Cloud**.
2. En la ventana que se abre, haga clic en **Propiedades**.
3. En la ventana **Configuración** que se abre, haga clic en el nombre del segmento que desee eliminar.
4. Haga clic en **Eliminar**.
5. En la ventana que se abre, haga clic en el botón **Aceptar** para confirmar su elección.

La conexión se eliminará. Los dispositivos del segmento de nube asociado a la conexión se eliminarán automáticamente de los grupos de administración.

Configuración de la programación de sondeo a través de Kaspersky Security Center Cloud Console

El sondeo de segmentos de nube se realiza siguiendo una programación. Si lo desea, puede configurar la frecuencia con la que se llevan a cabo los sondeos.

La frecuencia del sondeo está automáticamente configurada en cinco minutos por el Asistente de configuración del entorno de nube Puede cambiar este valor en cualquier momento y definir una programación diferente. Sin embargo, no se recomienda configurar el sondeo para que se ejecute con una frecuencia mayor a cada cinco minutos, porque esto podría dar lugar a errores en el funcionamiento de la API.

Para configurar la programación de sondeo para un segmento de nube:

1. En el menú principal, vaya a **Detección y despliegue** → **Detección** → **Cloud**.
2. En la ventana que se abre, haga clic en **Propiedades**.
3. En la ventana **Configuración** que se abre, haga clic en el nombre del segmento para el que quiera configurar la programación de sondeo.

   Se abre la ventana **Configuración de segmentos de la nube**.
4. En la ventana **Configuración de segmentos de la nube**, haga clic en **Programar sondeo**.

   Se abre la ventana **Programación**.
5. En la ventana **Programación**, configure los siguientes ajustes:

   - **Inicio programado**

     Opciones de programación para el sondeo:

     - Cada N días

       Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la fecha y hora indicadas. Cada sondeo estará separado del anterior por el número de días que indique.

       De forma predeterminada, se realizará un sondeo todos los días, a partir de la fecha y hora actuales del sistema.

     - Cada N minutos

       Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la hora indicada. Cada sondeo estará separado del anterior por el número de minutos que indique.

       De forma predeterminada, se realizará un sondeo cada cinco minutos, a partir de la hora actual del sistema.

     - Por días de la semana

       Se realizará un sondeo en forma periódica, a intervalos regulares, en el día de la semana y a la hora que indique.

       De manera predeterminada, el sondeo se ejecutará todos los viernes a las 18:00:00.

     - Cada mes en los días especificados de semanas seleccionadas

       Se realizará un sondeo en forma periódica, a intervalos regulares, en los días del mes y a la hora que indique.

       Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es las 18:00:00 p. m.

   - Intervalo de inicio (días)

     Indique a cuántos días o minutos, según el caso, equivale N.

   - Inicio desde

Indique cuándo se realizará el primer sondeo.

- **Ejecutar tareas no realizadas**

  Si su espacio de trabajo no está disponible durante el tiempo programado para el sondeo, Kaspersky Security Center Cloud Console puede iniciar el sonde inmediatamente después de que el espacio de trabajo esté disponible de nuevo o esperar a la próxima vez que el sondeo esté programado.

  Si esta opción está habilitada, Kaspersky Security Center Cloud Console comienza el sondeo inmediatamente después de que el espacio de trabajo vuelve a estar disponible.

  Si esta opción está desactivada, Kaspersky Security Center Cloud Console espera a la próxima vez que el sondeo esté programado.

  Esta opción está habilitada de manera predeterminada.

6. Haga clic en **Guardar** para guardar los cambios.

   La aplicación guarda la programación de sondeo para el segmento.

Ver los resultados del sondeo del segmento de la nube a través de Kaspersky Security Center Cloud Console

Puede consultar los resultados del sondeo de sus segmentos de nube. Dicho de otro modo, puede ver la lista de dispositivos de nube administrados por el Servidor de administración.

Para ver los resultados del sondeo de segmentos de nube:

En el menú principal, vaya a **Detección y despliegue** → **Detección** → **Cloud**.

Se muestran los segmentos de la nube disponibles para el sondeo.

Ver las propiedades de dispositivos de la nube a través de Kaspersky Security Center Cloud Console

Puede ver las propiedades de cada dispositivo de nube.

Para ver las propiedades de un dispositivo de nube:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados**.
2. Haga clic en el nombre del dispositivo en cuyas propiedades esté interesado.

   Se abrirá una ventana de propiedades con la sección **General** seleccionada.
3. Si desea ver las propiedades específicas de los dispositivos en la nube, seleccione la sección **Sistema** en la ventana de propiedades.

   Las propiedades que se muestran dependen de la plataforma de nube del dispositivo.

Para los dispositivos en AWS, se muestran las siguientes propiedades:

- **Dispositivo encontrado mediante API** (valor: **AWS**)
- **Región en la nube**
- **Cloud VPC**
- **Zona de disponibilidad en la nube**
- **Subred de nube**
- **Grupo de ubicación en la nube** (esta unidad se muestra solamente si la instancia pertenece a un grupo de ubicación)

Para los dispositivos en Azure, se muestran las siguientes propiedades:

- **Dispositivo encontrado mediante API** (valor: **Microsoft Azure**)
- **Región en la nube**
- **Subred de nube**

Para los dispositivos en Google Cloud, se muestran las siguientes propiedades:

- **Dispositivo encontrado mediante API** (valor: **Google Cloud**)
- **Región en la nube**
- **Cloud VPC**
- **Zona de disponibilidad en la nube**
- **Subred de nube**

Sincronización con la nube: Configuración de la regla de movimiento

Durante el funcionamiento del Asistente de configuración del entorno de nube, Sincronizar con Cloud se crea automáticamente. Esta regla le permite mover automáticamente las instancias detectadas en cada sondeo, desde el grupo Dispositivos no asignados al grupo Dispositivos administrados\Cloud para hacer que estos dispositivos queden disponibles para la administración centralizada. De manera predeterminada, una vez que se crea esta regla, se la deja habilitada. Puede deshabilitar, modificar o aplicar la regla en cualquier momento.

Para aplicar la regla "Sincronizar con la nube" o modificar sus propiedades:

1. En el menú principal, vaya a **Detección y despliegue → Despliegue y asignación → Reglas de movimiento**.

   Se abre una lista de reglas de movimiento.

2. En la lista de reglas de movimiento, seleccione **Sincronizar con subgrupo de la nube**.

   Se abre la ventana de propiedades de la regla.

3. De ser necesario, configure los siguientes ajustes en la pestaña **Segmentos de la nube** de la pestaña **Condiciones de reglas**:

- **El dispositivo está en un segmento de la nube**

  La regla solo se aplicará a los dispositivos que se encuentren en el segmento de nube seleccionado. De lo contrario, la regla se aplicará a todos los dispositivos que hayan sido detectados.

  Esta opción está seleccionada de manera predeterminada.

- **Incluir objetos secundarios**

  La regla se aplicará a todos los dispositivos del segmento seleccionado y a todas las subsecciones de nube anidadas. De lo contrario, la regla solo se aplicará a los dispositivos que estén en el segmento raíz.

  Esta opción está seleccionada de manera predeterminada.

- **Mover dispositivos desde objetos anidados a subgrupos correspondientes**

  Si esta opción está habilitada, los dispositivos de los objetos anidados se moverán automáticamente a los subgrupos que se correspondan con su estructura.

  Si esta opción está deshabilitada, los dispositivos de los objetos anidados se moverán automáticamente a la raíz del subgrupo "Cloud" y no habrá más ramificaciones.

  Esta opción está habilitada de manera predeterminada.

- **Crear subgrupos correspondientes a contenedores de dispositivos detectados recientemente**

  Si esta opción está activada, cuando la estructura del grupo **Dispositivos administrados\Cloud** no tiene subgrupos que coincidan con la sección que contiene el dispositivo, Kaspersky Security Center Cloud Console crea tales subgrupos. Por ejemplo, si se descubre una nueva subred durante la detección de dispositivos, se creará un nuevo grupo con el mismo nombre en el grupo **Dispositivos administrados\Grupo nube**.

  Si esta opción está desactivada, Kaspersky Security Center Cloud Console no crea ningún subgrupo nuevo. Si se descubre una nueva subred al sondear la red, por ejemplo, no se creará un nuevo grupo con el mismo nombre en el grupo **Dispositivos administrados\Cloud**, y los dispositivos que se encuentren en la subred detectada se moverán al grupo **Dispositivos administrados\Cloud**.

  Esta opción está habilitada de manera predeterminada.

- **Eliminar subgrupos para los que no se encontró coincidencia en los segmentos de la nube**

  Si esta opción está habilitada, la aplicación eliminará del grupo "Cloud" todo subgrupo que no tenga contraparte en un objeto de nube existente.

  Si esta opción está deshabilitada, se conservarán los subgrupos que no tengan contraparte en un objeto de nube existente.

  Esta opción está habilitada de manera predeterminada.

Si activó la opción **Sincronizar grupos de administración con estructura de nube** al usar el Asistente de configuración del entorno de nube, la regla **Sincronizar con subgrupo de la nube** se crea con las opciones **Crear subgrupos correspondientes a contenedores de dispositivos detectados recientemente** y **Eliminar subgrupos para los que no se encontró coincidencia en los segmentos de la nube** activadas.

Si no habilitó la opción **Sincronizar grupos de administración con estructura de nube**, la regla **Sincronizar con subgrupo de la nube** no tendrá estas opciones habilitadas. Si su trabajo con Kaspersky Security Center Cloud Console requiere que la estructura de los subgrupos en el subgrupo **Dispositivos administrados\Cloud** coincida con la estructura de los segmentos de la nube, active las opciones **Crear subgrupos correspondientes a contenedores de dispositivos detectados recientemente** y **Eliminar subgrupos para los que no se encontró coincidencia en los segmentos de la nube** en las propiedades de la regla y, luego, haga cumplir la regla.

4. En la lista desplegable **Dispositivo descubierto mediante la API**, seleccione uno de los siguientes valores:

   - **No**. Por algún motivo, el dispositivo no se puede detectar con la API de AWS, Azure o Google, es decir, o bien está fuera del entorno de nube o está en el entorno de nube pero no se puede detectar mediante la API.
   - **AWS**. El dispositivo se descubre mediante la API de AWS, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de AWS.
   - **Azure**. El dispositivo se descubre mediante la API de Azure, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Azure.
   - **Google Cloud**. El dispositivo se descubre mediante la API de Google, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Google.
   - Ningún valor. Este criterio no se puede aplicar.

5. Si es necesario, configure las propiedades de la regla en las demás secciones.

La regla de movimiento queda configurada.

Instalación remota de aplicaciones en máquinas virtuales de Azure

Debe tener una licencia válida para instalar aplicaciones en máquinas virtuales de Microsoft Azure.

Kaspersky Security Center Cloud Console admite los siguientes escenarios:

- Un dispositivo cliente se descubre mediante la API de Azure; la instalación también se realiza mediante una API. El uso de la API de Azure significa que solo puede instalar las siguientes aplicaciones:
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security para Windows
  - Kaspersky Security for Windows Server
- Un dispositivo cliente se descubre mediante la API de Azure; la instalación se realiza mediante puntos de distribución o, si no hay un punto de distribución, manualmente, mediante el uso de paquetes de instalación autónomos. De esta manera puede instalar cualquier aplicación compatible con Kaspersky Security Center Cloud Console.

Para crear una tarea para la instalación remota de la aplicación en máquinas virtuales de Azure:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Añadir**.

   Se inicia el Asistente para crear nueva tarea.

3. Siga las instrucciones del asistente:

   a. Seleccione **Instalar aplicación en remoto** como tipo de tarea.

   b. En la página **Paquetes de instalación**, seleccione **Instalación remota por API de Microsoft Azure**.

   c. Al seleccionar la cuenta para acceder a los dispositivos, use una cuenta de Azure existente o haga clic en **Añadir** e introduzca las credenciales de su cuenta de Azure:

   - **Nombre de cuenta Azure**

     Introduzca cualquier nombre para las credenciales que desea especificar. El nombre aparecerá en la lista de cuentas para ejecutar la tarea.

   - **Id. de la aplicación en Azure**

     Usted creó el id. de la aplicación en el portal de Azure.

     No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

   - **Contraseña de la aplicación Azure**

     Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

     Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

   d. Seleccione los dispositivos relevantes desde el grupo **Dispositivos administrados\Nube**.

Una vez que el asistente termina, la tarea para la instalación remota de la aplicación aparece en la lista de tareas.

Ponerse en contacto con el 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 Cloud Console o en alguna de las fuentes de información sobre Kaspersky Security Center Cloud Console, 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 Cloud Console.

Kaspersky proporciona asistencia técnica de Kaspersky Security Center Cloud Console durante su ciclo de vida (consulte la página del ciclo de vida de la asistencia técnica del producto). Antes de comunicarse con el servicio de soporte técnico, lea las reglas de soporte técnico.

Puede ponerse en contacto con el Servicio de soporte técnico de una de las siguientes maneras:

- Visitando el sitio web del Servicio de soporte técnico
- Enviando una solicitud al Servicio de soporte técnico desde el portal de Kaspersky CompanyAccount

Consultas mediante Kaspersky CompanyAccount al servicio de soporte técnico

Kaspersky CompanyAccount es un portal para las empresas que utilizan las aplicaciones Kaspersky. El portal Kaspersky CompanyAccount está diseñado para facilitar la interacción entre los usuarios y los especialistas de Kaspersky mediante solicitudes en línea. Puede usar Kaspersky CompanyAccount para hacer un seguimiento del estado de sus solicitudes en línea y almacenar un historial de dichas solicitudes.

Puede registrar a todos los empleados de su organización en una única cuenta de Kaspersky CompanyAccount. Esta cuenta única le permite administrar de forma centralizada las solicitudes electrónicas que envían los empleados registrados a Kaspersky, además de administrar los privilegios de estos empleados mediante Kaspersky CompanyAccount.

El portal Kaspersky CompanyAccount está disponible en los idiomas siguientes:

- 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.

Información necesaria para los especialistas del Soporte Técnico de Kaspersky

Cuando se ponga en contacto con los especialistas del Soporte Técnico de Kaspersky, es posible que le pidan la siguiente información:

- Información general sobre Kaspersky Security Center Cloud Console
- ID del espacio de trabajo
- Información de la licencia
- Cantidad de aplicaciones instaladas
- ID y estado del inquilino

Puede encontrar esta información en la sección del menú **Su cuenta** → **Servicio de soporte técnico**. Copie y comparta esta información para obtener ayuda sobre su problema.

Fuentes de información acerca de la aplicación

Página de Kaspersky Security Center Cloud Console en el sitio web de Kaspersky

En la página de Kaspersky Security Center Cloud Console en el sitio web de Kaspersky, puede consultar la información general de la aplicación, sus características y sus funciones.

La página de Kaspersky Security Center Cloud Console 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 Cloud Console de la Base de conocimientos, puede leer artículos que proporcionan información útil, recomendaciones y respuestas a preguntas frecuentes sobre cómo comprar, instalar y usar la aplicación.

Los artículos en la Base de conocimiento pueden proporcionar respuestas a preguntas relacionadas tanto con Kaspersky Security Center Cloud Console como con otras aplicaciones de Kaspersky. Estos artículos también pueden contener noticias vinculadas al soporte técnico.

Discutir las aplicaciones de Kaspersky con la comunidad

Si su pregunta no requiere una respuesta inmediata, puede analizarla con los expertos de Kaspersky y con otros usuarios en nuestro foro.

En el Foro, puede consultar temas de debate, publicar comentarios y crear temas nuevos.

> Se requiere una conexión a Internet para acceder a los recursos web.

Si no encuentra solución a su problema, comuníquese con el servicio de soporte técnico.

Problemas conocidos

Kaspersky Security Center Cloud Console tiene una serie de limitaciones que no son críticas para el funcionamiento de la aplicación:

- No es posible añadir un paquete de instalación con el mismo idioma de localización varias veces. Por ejemplo, si ya añadió el paquete de instalación de Kaspersky Endpoint Security para Windows (inglés), puede añadir paquetes de instalación de Kaspersky Endpoint Security para Windows localizados en otros idiomas, pero no en inglés.

- Cuando intenta activar la solución Kaspersky MDR, se produce un error si los servicios de MDR no están disponibles.

- En la directiva de Kaspersky Endpoint Security for Mac, en la sección **Protección avanzada contra amenazas**, si hace clic en el botón **Declaración de KSN** varias veces, la ventana que contiene la Declaración de KSN se abre tantas veces como haya hecho clic en el botón.

- En la ventana **Detalles de la alerta**, si hace clic en cualquier enlace que abre otra sección, y luego intenta regresar y hace clic en el botón **Atrás** de su navegador (o presiona **`Alt`** + **`Izquierda`**), la ventana **Detalles de la alerta** no se abre.

- Cuando intenta eliminar la última clave de licencia en la sección **Licencias de Kaspersky**, el botón **Eliminar** en la ventana de confirmación no está visible si el tema de la interfaz oscura de Web Console está activado.

- En la directiva de Kaspersky Endpoint Security for Mac, si activa la integración con KATA y no especifica la dirección del servidor y el certificado, un intento de activar la función Control web devuelve un error.

- 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.

- Una vez completada la tarea de *análisis de inventario* para un dispositivo Linux, se devuelve con error el intento de enviar los archivos recibidos a Kaspersky para su análisis.

- Si realiza un intento para iniciar sesión en Kaspersky Security Center Cloud Console usando Active Directory Federation Services (AD FS), pero no tiene los permisos requeridos, Kaspersky Security Center Cloud Console muestra el error de "Credenciales no válidas" en lugar de advertirle al usuario sobre los permisos que faltan.

- La tarea de Administrar dispositivos no funciona de manera correcta para dispositivos que ejecuten macOS.

- En la ventana Diagnóstico remoto, es posible que hacer clic en el botón **Descargar archivo completo** no dé como resultado una descarga correcta.

- Una vulnerabilidad de terceros ignorada (sin incluir el software de Microsoft) no se muestra en el diagrama de **Estadísticas de vulnerabilidades en dispositivos**.

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 las aplicaciones de Kaspersky, que incluye las actualizaciones críticas acumuladas durante cierto periodo de tiempo.

Administración centralizada de aplicaciones

Administración de aplicaciones remota usando los servicios de administración proporcionados en Kaspersky Security Center Cloud Console.

Administración directa de aplicaciones

Administración de aplicaciones mediante una interfaz local.

Administrador de Kaspersky Security Center Cloud Console

La persona que administra las operaciones de la aplicación a través del sistema de administración centralizada remota de Kaspersky Security Center Cloud Console.

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

Un componente de Kaspersky Security Center Cloud Console 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

Una aplicación antivirus de un desarrollador externo o una aplicación Kaspersky que no admite la administración a través de Kaspersky Security Center Cloud Console.

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 con información sobre las amenazas de seguridad informática conocidas por Kaspersky en el momento del lanzamiento de las bases de datos antivirus. Las entradas en las bases de datos antivirus permiten que se detecte código malicioso en los objetos analizados. Las bases de datos antivirus son generadas por los especialistas de Kaspersky. Se actualizan cada una hora.

Brote de virus

Serie de intentos deliberados de infectar un dispositivo con un virus.

Clave activa

Una clave que está siendo utilizada por la aplicación.

Clave de acceso de AWS IAM

Combinación formada por un id. de clave (una secuencia similar a "AKIAIOSFODNN7EXAMPLE") y una clave secreta (una secuencia similar a "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Este par de datos pertenece al usuario de IAM y se usa para obtener acceso a los servicios de AWS.

Clave de licencia adicional (o de reserva)

Una clave que certifica el derecho a usar la aplicación, pero que no se está utilizando en un momento dado.

Cloud Discovery

Cloud Discovery es un componente de la solución Cloud Access Security Broker (CASB) que protege la infraestructura de la nube de una organización. Cloud Discovery administra el acceso de los usuarios a los servicios en la nube. Los servicios en la nube incluyen, por ejemplo, Microsoft Teams, Salesforce, Microsoft Office 365. Los servicios en la nube se agrupan en categorías, por ejemplo, *Intercambio de datos*, *Mensajería*, *Correo electrónico*.

Complemento web de administración

Un componente especial que se utiliza para la administración remota del software Kaspersky a través de Kaspersky Security Center Cloud Console. Un complemento de administración es una interfaz entre Kaspersky Security Center Cloud Console y una aplicación específica de Kaspersky. El complemento de administración permite configurar tareas y directivas para esa aplicación.

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 de AWS

Interfaz web para ver y administrar los recursos de AWS. La Consola de administración de AWS está disponible en la Web, en https://aws.amazon.com/console/.

Cuarentena

Un repositorio especial que almacena archivos que probablemente están infectados con virus, así como los que no se pueden desinfectar en el momento de su detección.

Cuenta en Kaspersky Security Center Cloud Console

Una cuenta que debe tener para configurar Kaspersky Security Center Cloud Console, por ejemplo, para añadir y eliminar cuentas de usuario y configurar perfiles de seguridad (políticas de seguridad). Esta cuenta le permite usar el servicio My Kaspersky. Creará esta cuenta cuando comience a usar Kaspersky Security Center Cloud Console.

Directiva

Una directiva determina la configuración de una aplicación y controla la capacidad de configurar esa aplicación en los equipos de un grupo de administración. Se debe crear una directiva individual para cada aplicación. Aunque es posible crear múltiples directivas para las aplicaciones instaladas en los equipos de cada grupo de administración, solamente puede haber una directiva aplicada a cada aplicación dentro de cada grupo de administración.

Dispositivo administrado

Ordenador con Agente de red instalado o un dispositivo móvil con una aplicación de seguridad Kaspersky instalada.

Dispositivo con protección de UEFI

Dispositivo con una solución o aplicación Kaspersky para UEFI integrada a nivel de BIOS. La protección integrada garantiza que el dispositivo está protegido desde el momento en que se lo enciende. La protección en dispositivos sin software integrado, por el contrario, no comienza a funcionar sino hasta que la aplicación de seguridad se inicia.

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).

Espacio de trabajo

Una instancia de Kaspersky Security Center Cloud Console creada para una empresa específica. Cuando un cliente crea un espacio de trabajo, Kaspersky crea y configura la infraestructura y la Consola de administración basada en la nube que se requieren para administrar las aplicaciones de seguridad instaladas en los dispositivos de la empresa.

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.

Etiqueta de aplicación

Una etiqueta para aplicaciones de terceros que se puede utilizar para agrupar o encontrar aplicaciones. Una etiqueta asignada a las aplicaciones puede servir como una condición en las selecciones de dispositivos.

Etiqueta del dispositivo

Una etiqueta de un dispositivo que se puede utilizar para agrupar, describir o encontrar dispositivos.

Función de IAM

Conjunto de derechos para hacer solicitudes a servicios basados en AWS. Las funciones de IAM no están vinculadas a un usuario o grupo específicos; brindan derechos de acceso sin las claves de acceso de AWS IAM. Las funciones de IAM pueden asignarse a usuarios de IAM, instancias de EC2 y aplicaciones y servicios basados en AWS.

Gravedad de un evento

Propiedad de un evento registrado durante la ejecución de una aplicación de Kaspersky. Los niveles de gravedad posibles son los siguientes:

- Evento crítico
- Fallo operativo
- 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.

HTTPS

Protocolo seguro para transferir datos cifrados entre un navegador y un servidor web. HTTPS se usa para obtener acceso a información restringida, como datos corporativos o financieros.

Identity and Access Management (IAM)

Servicio de AWS que permite gestionar el acceso de los usuarios a otros servicios y recursos de AWS.

Imagen de máquina de Amazon (AMI)

Plantilla que contiene la configuración de software necesaria para ejecutar una máquina virtual. Cada AMI puede utilizarse para crear más de una instancia.

Instalación forzada

Método de instalación remota para las aplicaciones de Kaspersky. Permite instalar el software en dispositivos cliente específicos. Para que una instalación forzada se realice correctamente, la cuenta utilizada para la tarea debe tener los derechos necesarios para iniciar aplicaciones de manera remota en los dispositivos cliente. Este método se recomienda para instalar aplicaciones en dispositivos que ejecutan el sistema operativo Windows y admiten esta funcionalidad.

Instalación local

Método para instalar una aplicación de seguridad en un dispositivo conectado a una red corporativa. El método supone iniciar la instalación manualmente utilizando, o bien el paquete de distribución de la aplicación de seguridad, o bien un paquete de instalación publicado que se haya descargado en el dispositivo de antemano.

Instalación remota

Instalación de aplicaciones Kaspersky mediante servicios facilitados por Kaspersky Security Center Cloud Console.

Instancia de Amazon EC2

Máquina virtual creada con Amazon Web Services a partir de una imagen AMI.

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

Interfaz para programas de aplicación de la plataforma AWS que utiliza Kaspersky Security Center Cloud Console. En particular, las herramientas de la API de AWS se utilizan para el sondeo de segmentos de nube.

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 Next Expert View

Una aplicación diseñada para la ejecución centralizada de tareas básicas de administración y mantenimiento en la red de una organización. Kaspersky aloja Kaspersky Next Expert View y proporciona mantenimiento. La aplicación forma parte de la solución en la nube Kaspersky Next. Dentro de esta solución, también puede usar Kaspersky Next Pro View.

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 Network (KSN)

Infraestructura de servicios en la nube que proporciona acceso a la Base de datos de Kaspersky, que contiene información siempre actual sobre la reputación de los archivos, los recursos web y el software. Kaspersky Security Network permite que las aplicaciones de Kaspersky respondan más rápidamente a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de encontrarse con falsos positivos.

Lightweight Nagent (LWNGT)

Protocolo para la interacción con Kaspersky Endpoint Security en dispositivos móviles. El LWNGT (también llamado protocolo móvil) funciona como Agente de red sin instalar realmente el Agente de red en dispositivos móviles.

Network Location Awareness (NLA)

Servicio de Windows que ayuda a un sistema operativo a identificar la red en que se encuentra en un momento dado. NLA detecta cambios en la red y ajusta la configuración de seguridad del dispositivo.

Nivel de importancia del parche

Atributo del parche. Hay cinco niveles de importancia para los parches de Microsoft y de terceros:

- Crítico

- Máximo
- Medio
- Mínimo
- Desconocido

El nivel de importancia de un parche de terceros o de Microsoft está determinado por el nivel de gravedad menos favorable entre las vulnerabilidades que el parche debe reparar.

Operador de Kaspersky Security Center Cloud Console

Usuario que supervisa el estado y la operación de un sistema de protección administrada con Kaspersky Security Center Cloud Console.

Paquete de instalación

Un conjunto de archivos creados para la instalación remota de una aplicación de Kaspersky mediante el sistema de administración remota de Kaspersky Security Center Cloud Console. El paquete de instalación contiene una serie de ajustes que se necesitan para instalar la aplicación y ejecutarla inmediatamente una vez que concluye la instalación. La aplicación se configura con los ajustes predeterminados. El paquete de instalación se crea usando archivos con las extensiones .kpd y .kud que vienen incluidos en el kit de distribución de la aplicación.

Perfil de directiva

Un subconjunto con nombre de configuraciones de directiva. Este subconjunto se distribuye en dispositivos de destino junto con la directiva, y se complementa bajo una condición específica denominada Condición de activación del perfil.

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.

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 que tiene instalado el Agente de red y se utiliza para la distribución de actualizaciones, el sondeo de la red, la instalación remota de aplicaciones, la recopilación de información sobre equipos en un grupo de administración o dominio de difusión. El administrador selecciona los dispositivos apropiados y les asigna puntos de distribución de forma manual.

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 Cloud Console.

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.

Servidor de administración

Componente de Kaspersky Security Center Cloud Console que almacena de manera centralizada información sobre todas las aplicaciones de Kaspersky que están instaladas en la red corporativa. También puede utilizarse para administrar esas aplicaciones.

Servidor de administración doméstico

El Servidor de administración especificado durante la instalación del Agente de red. El Servidor de administración doméstico puede usarse en la configuración de los perfiles de conexión del Agente de red.

Servidor de administración virtual

Componente de Kaspersky Security Center Cloud Console diseñado para la administración del sistema de protección de la red de la organización cliente.

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

- Los Servidores de administración virtuales pueden funcionar solo como servidores de administración secundarios.
- El Servidor de administración virtual no permite la creación de Servidores de administración secundarios (incluidos los Servidores virtuales).

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.

Umbral de actividad viral

Cantidad máxima de eventos de un mismo tipo que se considera admisible en un tiempo limitado. Cuando se supera esta cantidad, se considera que ha habido un aumento en la actividad viral y que se corre el riesgo de enfrentar un brote de virus. Esta característica es importante durante los períodos de brotes de virus puesto que permite que los administradores respondan a tiempo a la amenaza de un ataque de virus.

Usuario de IAM

Usuario de servicios AWS. Un usuario de IAM puede tener derechos para sondear segmentos de nube.

Vulnerabilidad

Un error en un sistema operativo o en una aplicación que cualquier creador de malware puede aprovechar para penetrar en el sistema operativo o la aplicación y dañar su integridad. La presencia de una gran cantidad de vulnerabilidades en un sistema operativo lo hace poco confiable, ya que los virus que ingresan al sistema operativo pueden causar alteraciones tanto en el propio sistema operativo como en las aplicaciones instaladas.

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.

El archivo legal_notices.txt también se encuentra en la carpeta de instalación de Agente de red para Windows y Agente de red para Linux.

Para obtener información adicional sobre el código de terceros para los espacios de trabajo, consulte la documentación de Kaspersky Endpoint Security Cloud.

Avisos de marcas registradas

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos dueños.

Adobe, Acrobat, Flash, PostScript, Reader y Shockwave son marcas comerciales registradas o marcas comerciales de Adobe en los Estados Unidos o en otros países.

AMD64 es una marca comercial o una marca comercial registrada de Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS y AWS Marketplace son marcas comerciales de Amazon.com, Inc. o sus filiales.

Apache es una marca comercial registrada o una marca comercial de Apache Software Foundation.

Apple, App Store, AppleScript, FileVault, iPhone, iTunes, Mac, Mac OS, macOS, OS X, Safari y QuickTime 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, IOS y Cisco Jabber son marcas comerciales registradas o marcas comerciales de Cisco Systems, Inc. o sus filiales en los Estados Unidos y otros países determinados.

Citrix, XenServer son marcas comerciales registradas o marcas comerciales de Cloud Software Group, Inc. o sus subsidiarias en los Estados Unidos o en 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.

Corel y CorelDRAW son marcas comerciales o marcas comerciales registradas de Corel Corporation y/o de sus filiales en Canadá, los Estados Unidos y/u otros países.

Dropbox es una marca registrada de Dropbox, Inc.

Radmin es una marca comercial registrada de Famatech.

Firebird es una marca registrada de Firebird Foundation.

Foxit es una marca registrada de Foxit Corporation.

FreeBSD es una marca registrada de The FreeBSD Foundation.

Google, Android, Chrome, Dalvik, Firebase, Google Chrome, Google Earth, Google Maps, Google Play y Google Public DNS son marcas comerciales de Google LLC.

HUAWEI, HUAWEI CLOUD y EulerOS son marcas comerciales de Huawei Technologies Co., Ltd.

Intel y Core son marcas comerciales de Intel Corporation o sus subsidiarias.

IBM y QRadar son marcas comerciales de International Business Machines Corporation y están registradas en muchas jurisdicciones del mundo.

Node.js es una marca registrada de Joyent, Inc.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y en otros países.

Logitech es una marca comercial registrada o una marca comercial de Logitech en los Estados Unidos y/o en otros países.

Microsoft, Active Directory, ActiveSync, ActiveX, BitLocker, Excel, Hyper-V, InfoPath, Internet Explorer, Microsoft Edge, MS-DOS, MultiPoint, Office 365, OneNote, Outlook, PowerPoint, PowerShell, Segoe, Skype, SQL Server, Tahoma, Visio, Win32, Windows, Windows Azure, Windows Media, Windows Mobile, Windows Phone, Windows Server y Windows Vista son marcas comerciales del grupo de empresas de Microsoft.

CVE es una marca registrada de The MITRE Corporation.

Mozilla, Firefox y Thunderbird son marcas comerciales de la Fundación Mozilla en los Estados Unidos y en otros países.

Novell es una marca registrada de Novell Enterprises Inc. en los Estados Unidos y en otros países.

NetWare es una marca registrada de Novell Inc. en los Estados Unidos y en otros países.

OpenVPN es una marca registrada de OpenVPN, Inc.

Oracle, Java y JavaScript son marcas comerciales registradas de Oracle o sus filiales.

Parallels, el logotipo de Parallels y Coherence son marcas comerciales o marcas comerciales registradas de Parallels International GmbH.

Python es una marca comercial o una marca comercial registrada de Python Software Foundation.

Red Hat, Red Hat Enterprise Linux, CentOS y Fedora son marcas comerciales o marcas comerciales registradas de Red Hat, Inc. o sus subsidiarias en los 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.

SAMSUNG es una marca comercial de SAMSUNG en los Estados Unidos u otros países.

Debian es una marca registrada de Software in the Public Interest, Inc.

Splunk es una marca comercial y una marca comercial registrada de Splunk Inc. en los Estados Unidos y 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.

Rocky Linux es una marca registrada de The Rocky Enterprise Software Foundation.

UNIX es una marca registrada en los Estados Unidos y en otros países, licenciada exclusivamente a través de X/Open Company Limited.