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 usados 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 las aplicaciones
- 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 cantidad mínima de dispositivos para cada licencia
- Eventos sobre límites de licencia superados
- Métodos para distribuir los códigos de activación a los dispositivos administrados
- Agregar 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
- Ver información sobre las claves de licencia en uso agregadas al repositorio del Servidor de administración
- Ver información sobre las claves de licencia utilizadas para una aplicación de Kaspersky
- Eliminar una clave de licencia del Servidor de administración
- Eliminar una clave de licencia del repositorio
- Ver la lista de dispositivos en los que no está activada una aplicación de Kaspersky
- Revocar la aceptación de un Contrato de licencia de usuario final
- Renovación de licencias para aplicaciones de Kaspersky
- Usar Kaspersky Security Center Cloud Console una vez que caduca la licencia
- Terminología de las licencias
  - 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 transmitidos a los servidores de Kaspersky
Datos necesarios para el funcionamiento del espacio de trabajo
Datos necesarios para el funcionamiento de las aplicaciones administradas
Datos del usuario procesados en forma local
Acerca de los documentos legales de Kaspersky Security Center Cloud Console
Guía para reforzar la seguridad
Planificar la arquitectura de Kaspersky Security Center Cloud Console
Cuentas y autenticación
Administración de la protección de dispositivos cliente
Configurar 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 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
Crear una cuenta
Registro de una empresa y creación de un espacio de trabajo
Proteger más de 10 000 dispositivos
Apertura del espacio de trabajo en Kaspersky Security Center Cloud Console
Volver 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
Eliminación de un espacio de trabajo y una empresa
Cancelar la eliminación de un espacio de trabajo
Administración del acceso a la empresa y sus espacios de trabajo
Otorgamiento de acceso a su empresa y sus espacios de trabajo
Revocación del 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
Cambio de una dirección de correo electrónico
Cambio de una contraseña
Uso de la verificación en dos pasos
Acerca de la verificación en dos pasos
Escenario: Configuración de la verificación en dos pasos
Configuración de la verificación en dos pasos mediante SMS
Configuración de la verificación en dos pasos mediante una aplicación de autenticación
Cambio del número de teléfono móvil
Deshabilitación de la verificación en 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 DNS públicos
Escenario: Crear una jerarquía de servidores de administración que se administren con Kaspersky Security Center Cloud Console
Migración a Kaspersky Security Center Cloud Console
Acerca de la migración desde Kaspersky Security Center Web Console
Métodos para migrar a Kaspersky Security Center Cloud Console
Escenario: Migración sin una jerarquía de servidores de administración
Asistente de migración
Paso 1. Exportar los dispositivos administrados, los objetos y los ajustes de Kaspersky Security Center Web Console
Paso 2. Importar el archivo de exportación en Kaspersky Security Center Cloud Console
Paso 3. Reinstalar el Agente de red en los 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 al mover 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 desde Pro View a Expert View
Asistente de inicio rápido
Acerca del asistente de inicio rápido
Ejecución del asistente de inicio rápido
Paso 1. Selección de los paquetes de instalación que se van a 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. Cierre del asistente de inicio rápido
Despliegue inicial de las aplicaciones de Kaspersky
Escenario: Despliegue inicial de las aplicaciones de Kaspersky
Crear paquetes de instalación para las 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 el 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. Inicio de 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
Iniciar y detener aplicaciones de Kaspersky
Administración de dispositivos móviles
Funciones de detección y respuesta
Acerca de las funciones de detección y respuesta
Cambios en la interfaz tras 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
Configurar 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
Mover dispositivos o clústeres a un grupo de administración en forma manual
Configuración de reglas de retención para dispositivos no asignados
Configurar la protección de la red
Procedimiento: Configurar la protección de la red
Acerca de la administración de la seguridad centrada en el dispositivo y centrada en el usuario
Configuración y propagación de directivas: enfoque centrado en el dispositivo

Configuración y propagación de directivas: enfoque centrado en el usuario
Ajustes de la directiva del Agente de red
Comparación de la configuración de la directiva del Agente de red por sistemas operativos
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 dispositivos puntuales
Ajustes 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 del dispositivo
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
Sobre clústeres y conjuntos de servidores
Propiedades de un clúster o conjunto 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 archivos de 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 ver informes de 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
Asignar derechos de acceso a usuarios y grupos de seguridad
Asignación de un rol a un usuario o a un grupo de seguridad
Creación de roles de usuario
Editar un rol de usuario
Editar el alcance de un rol de usuario
Eliminar un rol de usuario
Asociación de perfiles de directivas con roles
Crear un grupo de seguridad
Editar un grupo de seguridad
Agregar cuentas de usuario a un grupo interno
Eliminar un grupo de seguridad
Configurar la integración de ADFS
Configurar la integración con Microsoft Entra ID
Habilitar el sondeo de Microsoft Entra ID
Agregar 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 regular de las bases de datos y las 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
Configurar los dispositivos administrados para que solo se actualicen mediante los puntos de distribución
Habilitar y deshabilitar la instalación automática de actualizaciones y parches para los componentes de Kaspersky Security Center Cloud Console
Instalación automática de actualizaciones para Kaspersky Endpoint Security para Windows
Acerca de los estados de las actualizaciones
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
Actualizar las bases de datos de Kaspersky Security for Windows Server
Administración de aplicaciones de terceros en dispositivos cliente
Limitaciones de la característica Administración de vulnerabilidades y parches
Características Administración de vulnerabilidades y parches disponibles en modo comercial, en modo de prueba y con distintas opciones de licencia
Acerca de las aplicaciones de terceros
Actualizaciones para el software de terceros
Procedimiento: Actualización de software de terceros
Instalación de actualizaciones para software de terceros
Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas
Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas
Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades
Agregar reglas de instalación de actualizaciones
Crear la tarea Instalar actualizaciones de Windows Update
Ver información sobre las actualizaciones disponibles para el software de terceros
Exportar la lista de actualizaciones de software disponibles a un archivo
Aprobar y rechazar actualizaciones de software de terceros
Actualización automática de aplicaciones de terceros
Encontrar y reparar 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: Buscar y reparar 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 instalados en los 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 para una aplicación de terceros usando la base de datos de Kaspersky
Ver y modificar la configuración de un paquete de instalación de una aplicación de terceros de la base de datos de Kaspersky
Configurar el paquete de instalación de una aplicación de terceros incluida en la base de datos de Kaspersky
Etiquetas de aplicación
Creación de una etiqueta de aplicación
Cambiar el nombre de una etiqueta de aplicación
Asignación de etiquetas a una aplicación
Quitarle una etiqueta a una aplicación
Eliminación de una etiqueta de aplicación
Configuración del Servidor de administración
Creación de una jerarquía de servidores de administración: agregar un Servidor de administración secundario
Configuración del plazo de almacenamiento para eventos vinculados a dispositivos eliminados
Combinación de correos electrónicos sobre eventos
Limitaciones para administrar servidores de administración secundarios instalados en una infraestructura local con 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
Procedimiento: Supervisión y generación de informes
Acerca de los tipos de funciones de supervisión y generación de informes
Panel y widgets
Uso del panel
Agregar widgets al panel
Ocultar un widget del panel
Mover un widget en el panel
Cambiar el aspecto o el tamaño de un widget
Cambiar la configuración de un widget
Acerca del modo solo panel
Configuración del modo solo panel
Informes
Utilización de informes
Crear una plantilla de informe
Ver y editar las propiedades de una plantilla de informe
Exportación de un informe a un archivo
Generar y ver un informe
Crear una tarea de entrega de informes
Eliminación de plantillas de informes
Eventos y selecciones de eventos
Acerca de los eventos de Kaspersky Security Center 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 Error funcional
Eventos del Servidor de administración: nivel Advertencia
Eventos del Servidor de administración: nivel Información
Eventos del Agente de red
Eventos del Agente de red: nivel Error funcional
Eventos del Agente de red: nivel Advertencia
Eventos del Agente de red: nivel Información
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
Recibir una advertencia sobre la caducidad de una licencia
Cloud Discovery
Habilitar Cloud Discovery mediante el widget
Agregar el widget de Cloud Discovery al panel
Ver información sobre el uso de servicios en la nube
Nivel de riesgo de un servicio en la nube
Bloquear el acceso a servicios en la nube no deseados
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
Configurar 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
Configurar Kaspersky Security Center Cloud Console para exportar eventos a un 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 los MSP
Escenario: Despliegue de la protección (administración de inquilinos mediante servidores de administración virtuales)
Escenario: Despliegue de la protección (administración de inquilinos mediante grupos de administración)
Uso conjunto de Kaspersky Security Center local y Kaspersky Security Center Cloud Console
Licencias de aplicaciones de Kaspersky para los MSP
Funciones de supervisión y de creación de informes para MSP
Cómo trabajar con Kaspersky Security Center Cloud Console en un entorno de nube
Opciones de licencia en un entorno de nube
Preparativos 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
Comprobar que Kaspersky Security Center Cloud Console tenga los permisos para trabajar con AWS
Creación de 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 para entornos de nube de 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 del segmento y configuración de la sincronización con la nube
Paso 5. Seleccionar una aplicación para crear una directiva y tareas
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 con Kaspersky Security Center Cloud Console
Agregar conexiones para sondear segmentos de nube a través de Kaspersky Security Center Cloud Console

Eliminar conexiones para el sondeo de segmentos de nube
Configurar la programación de sondeo con Kaspersky Security Center Cloud Console
Ver los resultados del sondeo de segmentos de nube en Kaspersky Security Center Cloud Console
Ver las propiedades de los dispositivos de nube en Kaspersky Security Center Cloud Console
Sincronización con la nube: Configuración de la regla de movimiento
Instalación remota de aplicaciones en máquinas virtuales de Azure
Contacto con el Servicio de 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 sobre 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 de 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)
Nagent ligero (LWNGT)
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
Subred de reconocimiento de ubicación de red (NLA)
Tarea
Tarea de grupo
Tarea local
Tarea para dispositivos específicos
Umbral de actividad viral
Usuario de IAM
Vulnerabilidad
Zona desmilitarizada (DMZ)
Información sobre 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 directivas y tareas para las aplicaciones de Kaspersky que respondan a los requisitos de la organización.
Requisitos de hardware y software Compruebe qué sistemas operativos y versiones de aplicaciones son compatibles.	**Aplicaciones de Kaspersky: actualización periódica 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 información sobre el funcionamiento de Kaspersky Security Center Cloud Console en modo de prueba y en modo comercial.	**Supervisión e informes** Visualice su infraestructura, vea los estados de protección de los dispositivos conectados a la red y acceda a información estadística para administrar el estado de protección de su organización. También puede utilizar informes.
Configuración inicial Comience a trabajar con su espacio de trabajo y 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 los grupos de administración y otros objetos relacionados que utilice en su despliegue local de Kaspersky Security Center a Kaspersky Security Center Cloud Console.	**Exportación de eventos a sistemas SIEM** Configure un mecanismo para exportar eventos a un sistema SIEM a través del protocolo Syslog.
Descubrimiento de dispositivos conectados a la red Descubra dispositivos nuevos y existentes en la red de su organización.	**Trabajo en un entorno de nube** Proteja máquinas virtuales en un entorno de nube de Amazon Web Services™, Microsoft Azure™ o Google™ Cloud Platform.
Ajuste de puntos de distribución y puertas de enlace de conexión Configure sus puntos de distribución.	**Guía de inicio rápido para proveedores de servicios administrados (MSP)** Aprenda a trabajar con Kaspersky Security Center Cloud Console si se desempeña como administrador en un 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 es compatible con las siguientes aplicaciones de Kaspersky:
  - Kaspersky Embedded Systems Security 3.4 para Linux
  - Kaspersky Endpoint Security 12.2 for Linux
  - Kaspersky Endpoint Security 12.8 para 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 agregar 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 de 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:

- Es 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 novedades y mejoras:

- Una nueva función de Cloud Discovery. Esta función le permite supervisar el uso de los servicios en la nube en los dispositivos administrados con Windows y bloquear el acceso a los servicios en la nube que considere no deseados. Cloud Discovery monitorea los intentos de los usuarios de acceder a estos servicios desde navegadores y aplicaciones de escritorio.
- Integración con Microsoft Entra ID para permitir que los usuarios de su organización inicien sesión en Kaspersky Security Center Cloud Console con las credenciales de su 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 computadoras 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 agregaron 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 la ejecución de la tarea**. Esta opción reduce el consumo de espacio en la base de datos del espacio de trabajo. El cambio solo afecta 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 agregar 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 utiliza.
- 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 agregan al área **Fijado** para un acceso rápido.
- Interfaz de la aplicación y experiencia del usuario optimizadas cuando selecciona la opción **Al completarse otra tarea** mientras programa una tarea.
- El informe de 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 novedades y mejoras:

- En la lista de dispositivos administrados, ahora puede seleccionar uno 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 agregó 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 novedades y mejoras:

- Ahora puede verificar la conexión con 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 de 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 for 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 porque estaban fuera del alcance de la funcionalidad de la aplicación:
  - Eventos de cifrado (**Operaciones** → **Protección y cifrado de datos** → **Eventos de cifrado**)
  - Intervalos IP (**Descubrimiento y despliegue** → **Descubrimiento** → **Intervalos IP**)
- Hemos actualizado el texto del Acuerdo de procesamiento de datos para Kaspersky Security Center Cloud Console.
- Varias versiones antiguas del navegador ya no son compatibles (Firefox ESR anterior a la versión 102).

Actualización de septiembre de 2023

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes novedades 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: junio de 2023

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

- Se lanzó una nueva Guía de sistema de protección. Le recomendamos que lea detenidamente la guía y que 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 para Mac.
- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Security 11.4 para Linux.
- Puede usar Kaspersky Security Center Cloud Console para exportar selecciones de eventos a un archivo y luego importar esas selecciones de eventos en 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 característica le permite asegurarse de que haya conectividad continua entre un dispositivo administrado y el Servidor de administración.

- La reorganización de la sección contiene configuraciones para integrar Kaspersky Security Center Cloud Console con otras aplicaciones de Kaspersky.

- Reorganización de la interfaz de usuario de la sección **Diagnóstico remoto**.

- 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 el uso, 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 novedades y mejoras:

- Kaspersky Security Center Cloud Console ahora admite clústeres y conjuntos de servidores como dispositivos administrados. Si se instala una aplicación de Kaspersky en un nodo de un clúster, el Agente de red enviará esa información al Servidor de administración. En Web Console, los clústeres y los conjuntos de servidores se muestran separados de los demás dispositivos administrados. Cada clúster o conjunto de servidores se administra como si se tratara de un objeto individual e indivisible.

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

- El número máximo de entradas que puede incluir un informe se incrementó hasta 2500 para un informe en Web Console y hasta 10 000 para un informe que exporta a un archivo.

- Ahora puede elegir si desea o no incluir los dispositivos administrados con el estado Sin inconvenientes en el informe de estado de la 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 publicó 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 característica le permite redistribuir y optimizar el tráfico de 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 basado en Linux y transmitirla al Servidor de administración.

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

Actualización de noviembre de 2022

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes novedades 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 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 videos en la sección **Presentación y tutoriales**.

Actualización de octubre de 2022

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

- Ahora puede asignar administradores dedicados para 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 los 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 admitido: Kaspersky Security Center Cloud Console se ha traducido completamente al japonés.

Actualización de julio de 2022

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

- Nuevas versiones de las aplicaciones de Kaspersky compatibles:
  - Kaspersky Endpoint Agent 3.13
  - Kaspersky Endpoint Security 11.2.1 for Mac
  - Kaspersky Security para iOS: 1.0.0
  - Kaspersky Endpoint Security 11.10.0 para Windows
- Hemos actualizado el contenido del Contrato y del Acuerdo de procesamiento de datos de Kaspersky Security Center Cloud Console.
- Nuevo idioma admitido: la infraestructura de Kaspersky Security Center Cloud Console ahora está disponible en japonés. Pronto también admitiremos el idioma japonés dentro de los espacios de trabajo de Kaspersky Security Center Cloud Console.

Actualización de abril de 2022

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes novedades 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.

Actualizado el 09 de marzo de 2022

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

- Implementación de la Integración con Kaspersky Endpoint Detection and Response Expert.
- Implementación de 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.

Actualizado el 11 de febrero de 2022

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

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

Actualización: 10 de diciembre de 2021

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

- Mejoras para operar con usuarios internos:
  - Ahora puede agregar usuarios internos nuevos a través del portal.
  - La aplicación ahora le impedirá quitarse derechos a usted mismo.

Actualizado el lunes, 18 de octubre de 2021

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

- Kaspersky Security Center Cloud Console ahora es compatible con Kaspersky Endpoint Detection and Response Optimum 2.0.
- Ahora puede administrar los dispositivos móviles con Android a través de Kaspersky Security Center Cloud Console.
- Kaspersky Marketplace está disponible como una nueva sección del menú: ahora puede buscar una aplicación de Kaspersky a través de Kaspersky Security Center Cloud Console.
- Hay una nueva sección disponible en el menú, Novedades de Kaspersky. Allí encontrará información actualizada sobre las aplicaciones de Kaspersky que estén instaladas en los dispositivos administrados. Kaspersky Security Center Cloud Console actualiza periódicamente la información de esta sección.
- Ahora puede administrar servidores de administración secundarios con sistemas operativos Linux a través de Kaspersky Security Center Cloud Console.

Actualizado el 7 de septiembre de 2021

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes novedades 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 es compatible con los entornos de nube de Amazon Web Services, Microsoft Azure y Google Cloud. Para proteger instancias o máquinas virtuales en un entorno de nube, necesitará una de las licencias de Kaspersky Hybrid Cloud Security. La aplicación ofrece un Asistente de configuración para entornos de nube.

- Cada espacio de trabajo admite ahora un máximo de 25 000 dispositivos.

- A partir de ahora, Kaspersky Security Center Cloud Console puede integrarse con un sistema SIEM. Puede exportar eventos a un sistema 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 y sus propias directivas, tareas, informes y eventos. Puede usar servidores de administración virtuales para administrar organizaciones cliente que tengan flujos de trabajo complejos desde su espacio de trabajo. Tenga en cuenta que los servidores de administración virtuales creados en un despliegue local de Kaspersky Security Center no pueden migrarse a Kaspersky Security Center Cloud Console.

- Ahora puede modificar el ancho de las columnas de las tablas. También puede buscar datos y ordenarlos.

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

Actualizado el 27 de octubre de 2020

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes novedades 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).

- A partir de ahora, puede usar las siguientes licencias:

  - Kaspersky Endpoint Detection and Response Optimum

  - Kaspersky Endpoint Security for Business Advanced

  - Kaspersky Total Security for Business

- Se han implementado las siguientes funciones:

  - Administración de vulnerabilidades y parches

  - Administración de cifrado

  - Control de aplicaciones

  - Control de anomalías adaptativo

  - Sesiones de RDP y de Windows Desktop Sharing

- El menú de navegación ahora es vertical. Se asemeja al que ofrece Kaspersky Security Center en su interfaz basada en Microsoft Management Console.

- Se han publicado videos técnicos de capacitación que le permitirán aprender sobre el funcionamiento de la aplicación.

Actualizado el 30 de junio de 2020

Esta actualización de Kaspersky Security Center Cloud Console incluye las siguientes novedades 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 han realizado mejoras en el Asistente de inicio rápido: se eliminaron algunos pasos, se modificó ligeramente la secuencia de pasos y se editaron algunos textos para que fueran más fáciles de comprender.
- 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 administrada de Kaspersky 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 que se lo elimine, de forma predeterminada, se lo eliminará automáticamente en un plazo de siete días. De ser necesario, puede hacer que el espacio de trabajo se elimine en forma inmediata.
- Se ha implementado un mecanismo de verificación en dos pasos para iniciar sesión en la consola.

Kaspersky Security Center Cloud Console

Esta sección contiene información sobre el objetivo de Kaspersky Security Center Cloud Console y sus funciones 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 un equipo o servidor propios. A través de Kaspersky Security Center Cloud Console, el administrador puede instalar las aplicaciones de seguridad de Kaspersky en los dispositivos de una red corporativa, ejecutar tareas de análisis y actualización en forma remota y gestionar las directivas de seguridad de las aplicaciones administradas. También puede usar un panel detallado para conocer rápidamente los estados de los dispositivos corporativos, consultar informes detallados y acceder a ajustes pormenorizados en las directivas de protección.

Acerca de Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console es una aplicación diseñada para administradores de redes corporativas y personas que tienen a su cargo la protección de dispositivos en organizaciones de muy diversos tipos.

Kaspersky Security Center Cloud Console permite hacer lo siguiente:

- Instalar aplicaciones de Kaspersky en los dispositivos de una red y administrar las 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 virtuales y organizarlos en una jerarquía.
- Proteger estaciones de trabajo, servidores y otros dispositivos conectados a la red:
  - Administrar un sistema de protección antimalware basado en las aplicaciones de Kaspersky.
  - Usar prestaciones de detección y respuesta (EDR y MDR) para fines como los siguientes (si se cuenta con una licencia de Kaspersky Endpoint Detection and Response o de Kaspersky Managed Detection and Response):
    - Analizar e investigar incidentes
    - Crear un gráfico con la cadena de desarrollo de la amenaza para visualizar un incidente
    - Aceptar o rechazar respuestas manualmente o configurar la aceptación automática de todas las respuestas
- Usar Kaspersky Security Center Cloud Console como aplicación multiinquilino.
- Administrar de forma remota las aplicaciones de Kaspersky instaladas en los dispositivos cliente.
- Realizar un despliegue centralizado de claves de licencia para las aplicaciones de Kaspersky instaladas en los dispositivos cliente.
- Crear y administrar directivas de seguridad para los dispositivos conectados a la red.
- Crear y administrar cuentas de usuario.

- Crear y administrar roles de usuario (RBAC).
- Crear y administrar tareas para las aplicaciones instaladas en los dispositivos de red.
- Ver informes sobre el estado del sistema de seguridad de cada organización cliente en particular.

Para administrar Kaspersky Security Center Cloud Console, se utiliza una Consola de administración basada en la nube. Esta consola permite que el dispositivo del administrador interactúe con 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 utiliza un navegador para conectarse a Kaspersky Security Center Cloud Console, el navegador establece una conexión con el Servidor de Kaspersky Security Center Cloud Console.

El Servidor de administración y el sistema de administración de bases de datos (DBMS, por sus siglas en inglés) conectado a este se encuentran instalados en un entorno de nube y se le ofrecen a usted como servicio. El mantenimiento del Servidor de administración y del DBMS se proporciona como parte del servicio. Los componentes de software de Kaspersky Security Center Cloud Console se mantienen siempre actualizados. A fin de resguardar la información, se crean copias de seguridad periódicas tanto del Servidor de administración como de los objetos creados (directivas, tareas, etc.).

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 utilizar Kaspersky Security Center Cloud Console como cliente, solo necesita un navegador.

Solo puede usar una única ventana o pestaña del navegador para trabajar con Kaspersky Security Center Cloud Console.

La resolución de pantalla mínimas es 1366x768 píxeles.

Los requisitos de hardware y software con los que debe cumplir el dispositivo son los que impone el 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
- Versión de soporte extendido de Mozilla Firefox 128.8.0 o versiones posteriores

Agente de red

Requisitos de hardware mínimos:

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

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

- CPU con una frecuencia operativa de 1.4 GHz o superior Se requiere un SO 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 o 64 bits) Microsoft Windows 10 TH2 (noviembre de 2015) Home/Pro/Pro for Workstations/Enterprise/Education (32 o 64 bits) Microsoft Windows 10 RS1 (agosto de 2016) Home/Pro/Pro for Workstations/Enterprise/Education (32 o 64 bits) Microsoft Windows 10 RS2 (abril de 2017) Home/Pro/Pro for Workstations/Enterprise/Education (32 o 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 bits o 64 bits)

	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) (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 (64 bits) CentOS Stream 9 (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)
- KVM (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 distintos productos otorgan acceso a diversos tipos de aplicaciones y soluciones de Kaspersky.

Las siguientes aplicaciones y soluciones de Kaspersky pueden desplegarse y administrarse 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 for 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 para 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 una aplicación en un dispositivo administrado, pero no actualiza la directiva correspondiente y continúa utilizando una directiva obsoleta con la nueva versión, la aplicación seguirá brindándole datos a Kaspersky Security Center Cloud Console. Sin embargo, Kaspersky Security Center Cloud Console no podrá procesar esos datos según lo descrito en la sección Datos procesados de las aplicaciones administradas de la documentación. Para que Kaspersky Security Center Cloud Console pueda procesar estos datos, deberá 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 usar Kaspersky Security Center de las siguientes maneras:

- Como solución de nube

  Kaspersky Security Center se instalará por usted en un entorno de nube. Kaspersky le dará 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 solución desplegada en una infraestructura local (con base Windows o base Linux)

  Usted se encargará de instalar Kaspersky Security Center en un dispositivo local. Para administrar el sistema de seguridad de su red, utilizará la Consola de administración basada en Microsoft Management Console o Kaspersky Security Center Web Console.

  Además de la aplicación para Windows, puede utilizar Kaspersky Security Center Linux. Pensada para entornos en los que solo se utiliza Linux, Kaspersky Security Center Linux se ha diseñado para desplegar y administrar la protección de dispositivos Linux a través de un Servidor de administración instalado en Linux. Kaspersky Security Center basado en Windows y Kaspersky Security Center Linux tienen diferentes conjuntos de características.

Utilice la siguiente tabla para comparar las características principales de Kaspersky Security Center y Kaspersky Security Center Cloud Console.

Comparación de las características de Kaspersky Security Center como solución local y como solución de nube

Característica o propiedad	Kaspersky Security Center cuando se ejecuta de forma local	Kaspersky Security Center Cloud Console
Ubicación del Servidor de administración	Local	En la nube
Ubicación del sistema de administración de bases de datos (DBMS)	Local	En la nube
Consola de administración web	✓	✓
Mantenimiento del Servidor de administración y del DBMS	A cargo del cliente	A cargo de Kaspersky
Jerarquía de Servidores de administración	✓	✓ (El Servidor de administración de Kaspersky Security Center Cloud Console solo puede actuar como Servidor de administración principal en la jerarquía y solo puede usarse para supervisar tareas y directivas)
Jerarquía de grupos de administración	✓	✓
Migración de los dispositivos administrados y los objetos relacionados de Kaspersky Security Center local a Kaspersky Security Center Cloud Console	✓	✓
Sondeo de red	✓	✓ (solo a través de los puntos de distribución)
Número de dispositivos administrados	100000	25000
Protección de dispositivos administrados con Windows, Linux y macOS	✓	✓
Protección de dispositivos móviles	✓	✓ (solo se admiten Kaspersky Endpoint Security para Android y Kaspersky Security para iOS)

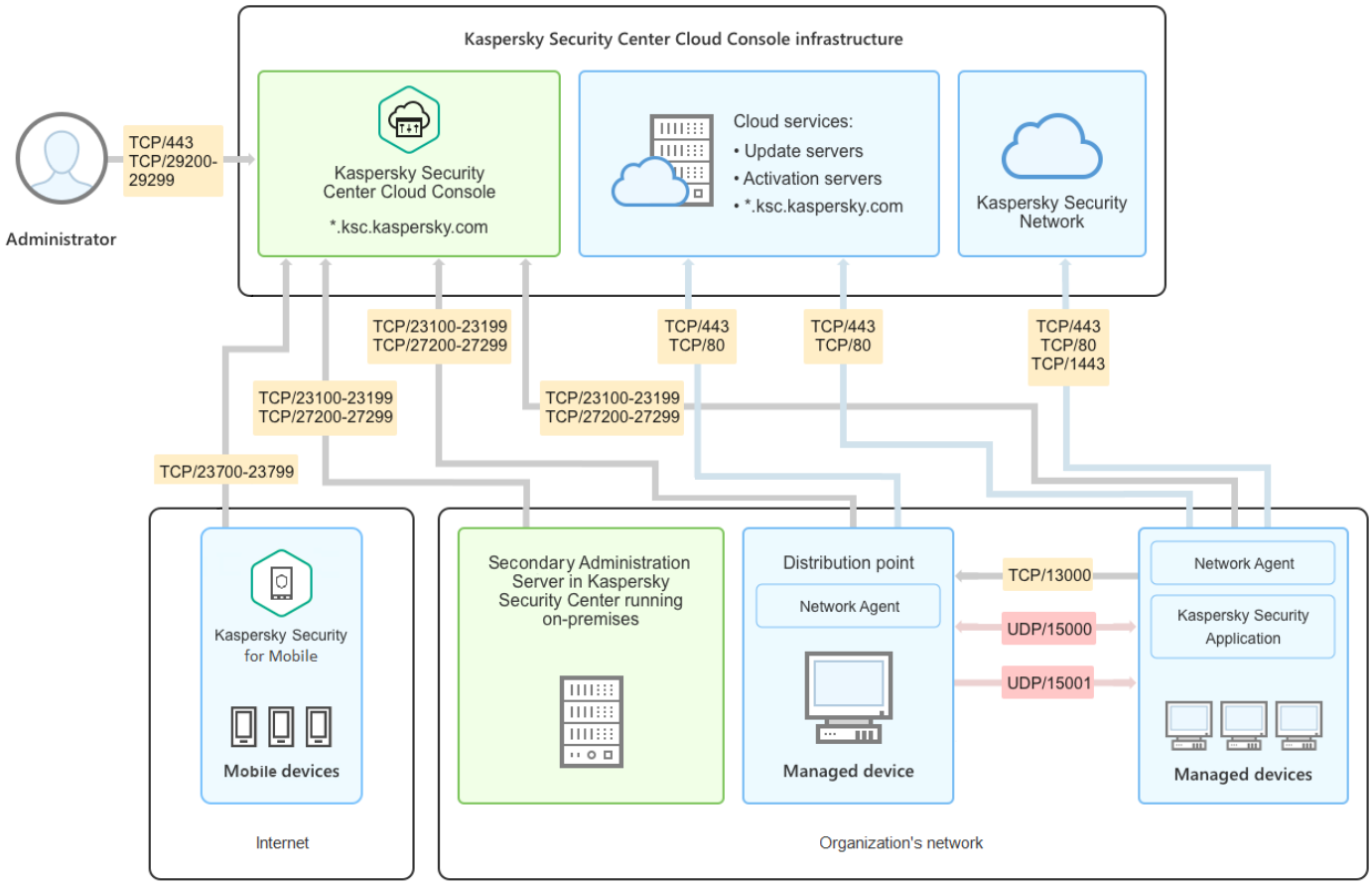
Protección de infraestructuras de nubes públicas	✓	✓
Administración de la seguridad centrada en el dispositivo	✓	✓
Directivas para aplicaciones	✓	✓
Tareas para aplicaciones de Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
Servidor proxy de KSN	✓	✓ (solo en puntos de distribución)
Kaspersky Private Security Network	✓	—
Implementación centralizada de claves de licencia para aplicaciones de Kaspersky	✓	✓
Traspaso de dispositivos administrados a otro Servidor de administración	✓	— (se debe reinstalar el Agente de red en los dispositivos administrados para pasarlos 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 los eventos ocurridos en los dispositivos administrados	✓	✓
Creación y gestión de cuentas de usuario	✓	✓
Número máximo de eventos en la base de datos	400000 (se puede aumentar hasta 45000000)	400000 (depende del número de dispositivos administrados)
Integración con sistemas SIEM	✓	✓ (utilizando solo el formato Syslog y TLS sobre el protocolo TCP)
Usar Servidor de administración como un servidor WSUS	✓	—
Supervisar los estados de directivas 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

En esta sección se describen los componentes de Kaspersky Security Center Cloud Console y el modo en que interactúan.



Arquitectura de Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console se administra mediante una consola de nube y consta de 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 en la 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**. Aquí se incluyen los servidores de actualización y los servidores de activación.
- **Kaspersky Security Network (KSN)**. Servidores que contienen una base de datos en la que se detalla la reputación de los archivos, los recursos web y el software. Kaspersky actualiza la información de esta base de datos continuamente. Kaspersky Security Network permite que las aplicaciones de Kaspersky respondan más

rápido a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de enfrentar falsos positivos.

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

- **Punto de distribución**. Equipo en el que se ha instalado el Agente de red y que se utiliza para distribuir actualizaciones, realizar sondeos de red, instalar aplicaciones en forma remota y recopilar información sobre los equipos asociados a un grupo de administración o a un dominio de difusión. Es tarea del administrador determinar qué dispositivos actuarán como puntos de distribución y designarlos como tales manualmente.

- **Dispositivos administrados**. Computadoras de la red del cliente que se encuentran protegidas con Kaspersky Security Center Cloud Console. Cada dispositivo administrado debe contar con el Agente de red y una aplicación de seguridad de Kaspersky.

- **Servidor de administración secundario instalado en la infraestructura local** (opcional). Puede usar un Servidor de administración local para crear una jerarquía de servidores de administración.

Puertos usados por Kaspersky Security Center Cloud Console

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

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

Puerto (o intervalo de puertos)	Protocolo	Objetivo del puerto (o del intervalo de puertos)
23100-23199	TCP/TLS	Recepción de conexiones de los agentes de red y los servidores de administración secundarios en el Servidor de administración de Kaspersky Security Center Cloud Console alojado en *.ksc.kaspersky.com. La infraestructura de Kaspersky puede usar cualquier puerto que se encuentre en este intervalo y cualquier dirección web alcanzada por esta máscara. El puerto y la dirección web pueden cambiar ocasionalmente.
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 alojado en *.ksc.kaspersky.com. La infraestructura de Kaspersky puede usar cualquier puerto que se encuentre en este intervalo y cualquier dirección web alcanzada por esta máscara. El puerto y la dirección web pueden cambiar ocasionalmente.
27200-27299	TCP/TLS	Recepción de conexiones establecidas por los dispositivos administrados (excepto los dispositivos móviles) para la activación de aplicaciones. Conexión al Servidor de administración de Kaspersky Security Center Cloud Console alojado en *.ksc.kaspersky.com. La infraestructura de Kaspersky puede usar cualquier puerto que se encuentre en este intervalo y cualquier dirección web alcanzada por esta máscara. El puerto y la dirección web pueden cambiar ocasionalmente.
29200-29299	TCP/TLS	Túneles de conexión establecidos con la utilidad klsctunnel para comunicarse con los dispositivos administrados a través del Servidor de administración de Kaspersky Security Center Cloud Console alojado en *.ksc.kaspersky.com. La infraestructura de Kaspersky puede usar cualquier puerto que se encuentre en este intervalo y cualquier dirección web alcanzada por esta máscara. El puerto y la dirección web pueden cambiar ocasionalmente.
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 con 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 de las puertas de enlace de conexión (si se las utiliza)	Administración de dispositivos cliente
15000	Difusión UDP	Obtención de datos sobre otros agentes de red asociados al mismo dominio de difusión	Transmisión 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 nuevas versiones de software de terceros. Las recomendaciones descritas para configurar puertos se basan en las experiencias de Soporte técnico y en nuestras prácticas recomendadas.

La siguiente tabla enumera los puertos adicionales que deben estar abiertos en los dispositivos cliente que tienen el Agente de red instalado como 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 transmisión de actualizaciones y paquetes de instalación
13111 (solo si el servicio del 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 del 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 del 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 lo instaló de forma local. Use esos puertos para permitir la interacción entre los dispositivos cliente y su Servidor de administración secundario (o servidores de administración secundarios).

Conceptos básicos

En esta sección se explican los conceptos básicos relacionados con Kaspersky Security Center Cloud Console.

Agente de red

La interacción entre el Servidor de administración y los dispositivos está a cargo del componente *Agente de red* de Kaspersky Security Center Cloud Console. Si un dispositivo tiene instalada una aplicación de Kaspersky que se administra mediante Kaspersky Security Center Cloud Console, debe tener instalado, también, el Agente de red.

El Agente de red es un servicio que se instala en el dispositivo con los siguientes atributos:

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

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

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 gestionados.

Grupos de administración

Un *grupo de administración* (de ahora en adelante *grupo*) es un conjunto lógico de dispositivos administrados que se combinaron en función de un rasgo específico para que se los pueda administrar como una única unidad 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 principal-secundario. Cada Servidor de administración puede tener varios servidores de administración secundarios, ubicados en diferentes niveles de anidamiento de esta jerarquía. No existe un límite en cuanto al nivel de anidamiento para los servidores de administración secundarios. Los grupos de administración del Servidor de administración principal incluyen los dispositivos cliente de todos los servidores de administración secundarios.

El Servidor de administración de Kaspersky Security Center Cloud Console solo puede actuar como Servidor de administración principal. Sus servidores secundarios solo pueden ser servidores de administración instalados en una infraestructura local.

A la hora de migrar de un Servidor de administración local al Servidor de administración de Kaspersky Security Center Cloud Console, puede organizar los servidores de administración en una jerarquía. Luego, para facilitar la migración, puede ceder el control de solo parte de los dispositivos administrados al Servidor de administración de Kaspersky Security Center Cloud Console. El Servidor de administración local seguirá estando a cargo de los dispositivos administrados restantes. Esta estrategia le permitirá probar las características de administración de Kaspersky Security Center Cloud Console con un número limitado de dispositivos administrados. Al mismo tiempo, podrá configurar directivas, tareas, informes y otros objetos para hacer pruebas de administración y control en toda su red. Con esto, si resultara necesario, podrá volver a utilizar los objetos configurados en el Servidor de administración local.

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. Utilice la función que permite buscar dispositivos en los grupos de administración de diferentes servidores de administración utilizando sus atributos de red.

Servidor de administración virtual

El Servidor de administración virtual (también llamado *Servidor virtual*) es un componente de Kaspersky Security Center Cloud Console cuyo propósito es administrar la protección antivirus de la red de la organización cliente. Cada Servidor de administración virtual puede tener su propia estructura de grupos de administración y sus propios instrumentos de gestión y supervisión (directivas, tareas, informes, eventos, etc.). Las prestaciones que ofrecen los servidores de administración virtuales pueden ser de utilidad en organizaciones con flujos de trabajo complejos.

Los servidores de administración virtuales tienen las siguientes restricciones:

- Los servidores de administración virtuales solamente se pueden utilizar en el modo comercial de Kaspersky Security Center Cloud Console.
- Los servidores de administración virtuales no admiten la creación de servidores de administración secundarios (sean o no virtuales).
- Los servidores de administración virtuales de Kaspersky Security Center no se pueden migrar a Kaspersky Security Center Cloud Console.
- Los servidores de administración virtuales no pueden tener un administrador dedicado. De manera predeterminada, la persona que administra el Servidor de administración principal tiene también a su cargo los

servidores 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 los servidor de administración virtuales, el número de secciones está restringido.

Punto de distribución

Un *punto de distribución* es un dispositivo con el Agente de red instalado que se utiliza para distribuir actualizaciones, instalar de forma remota las aplicaciones y recuperar la información relativa a los dispositivos en red.

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

Un punto de distribución puede realizar las siguientes funciones:

- Distribuir actualizaciones y paquetes de instalación a los dispositivos cliente dentro del grupo (incluida la distribución a través de multidifusión mediante UDP). El punto de distribución puede recibir las actualizaciones de los servidores de actualizaciones de Kaspersky utilizando una tarea de actualización creada para el mismo.

  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.
- Permitir la instalación remota de software de terceros y de aplicaciones de Kaspersky utilizando herramientas de Microsoft Windows, incluso en dispositivos cliente que no tienen el Agente de red.

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

- Actuar como servidor proxy asociado a Kaspersky Security Network.

  Esta característica no estará disponible si el dispositivo que actúa como punto de distribución utiliza un sistema operativo 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. El uso de HTTP o HTTPS en lugar de SOAP reduce el volumen de tráfico y, de ese modo, permite mejorar el rendimiento.

Los dispositivos con el Agente de red instalado deben designarse como puntos de distribución de los grupos de administración en forma manual. 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. Se debe destacar, sin embargo, que el dispositivo que actúa como punto de distribución no necesariamente tiene que formar parte del grupo de administración para el que ha sido designado. 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 de multidifusión IP única, diferente de todas las otras direcciones. Con ello se evitan las sobrecargas de red que podrían registrarse si las direcciones IP se superpusieran.

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

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

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

Para ejecutar tareas de instalación remota en un dispositivo designado como punto de distribución, se requiere espacio en disco adicional. El volumen de espacio libre debe superar el tamaño total de los paquetes de instalación que se instalarán.

Para ejecutar tareas de actualización (instalación de parches) y de reparación de vulnerabilidades en un dispositivo designado como punto de distribución, se requiere espacio en disco adicional. El volumen de espacio libre debe ser de al menos el doble del tamaño total de los parches que se instalarán.

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

Complemento web de administración

Para administrar el software de Kaspersky en forma remota a través de Kaspersky Security Center Cloud Console, se utiliza un componente especial, llamado *complemento web de administración*. En lo sucesivo, el término *complemento de administración* hará referencia a un complemento web de administración. Un complemento de administración es una interfaz entre Kaspersky Security Center 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
- Brinda las funciones de Kaspersky Security Center Cloud Console que permiten mostrar los eventos y los datos de funcionamiento de una aplicación, así como las estadísticas transmitidas por los dispositivos cliente

Directivas

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

Estado de la directiva

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

Las directivas funcionan de acuerdo con las siguientes reglas:

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

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

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

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

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

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

Perfiles de directivas

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

Para evitar la creación de varias instancias de una sola directiva, Kaspersky Security Center Cloud Console 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 las aplicaciones

En esta sección, encontrará información relacionada con las licencias de las aplicaciones.

Licencias de Kaspersky Security Center Cloud Console

Al concluir este escenario, podrá comenzar a usar Kaspersky Security Center Cloud Console y sus aplicaciones de seguridad administradas con una licencia.

Kaspersky Security Center Cloud Console le brinda una ubicación central para distribuir claves de licencia a las aplicaciones de Kaspersky instaladas en los dispositivos cliente, monitorear el uso de esas claves de licencia y renovar las licencias de las aplicaciones.

Si ya está utilizando Kaspersky Security Center Cloud Console, puede visitar Kaspersky Marketplace para ver todo el catálogo de soluciones empresariales que ofrece Kaspersky, seleccionar las soluciones que necesite y adquirirlas en el sitio web de Kaspersky.

El modo de prueba: descubra las funciones de Kaspersky Security Center Cloud Console antes de comprar una licencia

Antes de nada, puede probar Kaspersky Security Center Cloud Console en forma gratuita. Para ello, cree un espacio de trabajo de prueba que terminará en 30 días. Si necesita un espacio de trabajo comercial sin límites de vigencia, compre una licencia.

No es posible pasar del modo de prueba al modo comercial. Los espacios de trabajo de prueba se eliminan automáticamente, junto con todo su contenido, cuando se llega al límite de treinta días.

Etapas

El escenario se divide en etapas:

1. **Obtener un código de activación para usar Kaspersky Security Center Cloud Console con una licencia en modo comercial. Comprar una o más licencias**

   Las distintas licencias brindan acceso a distintas aplicaciones y servicios de Kaspersky, por lo que posiblemente quiera comprar más de una licencia.

   Descubra cuáles son las licencias que puede comprar y cuál es el mínimo de dispositivos que exige cada licencia.

   Kaspersky Security Center Cloud Console forma parte de varias soluciones de Kaspersky. Elija la solución que usará y compre una licencia para la misma. 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 esta tabla para ver las funciones de Administración de vulnerabilidades y parches a las que brinda acceso cada licencia.

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

   Si opera como proveedor de servicios administrados (MSP), consulte el tema sobre las licencias de Kaspersky Security Center Cloud Console para MSP.

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

La clave de licencia para activar Kaspersky Security Center Cloud Console se ingresa al momento de crear un espacio de trabajo.

Si tiene más de una clave de licencia, ingrese una al azar; más adelante, deberá agregar otras claves de licencia en Kaspersky Security Center Cloud Console para activar las aplicaciones de Kaspersky administradas.

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

   Las claves de licencia que se van a desplegar deben agregarse primero al repositorio del Servidor de administración.

   La clave de licencia ingresada al crear el espacio de trabajo se agrega al repositorio del Servidor de administración automáticamente.

   Si tiene claves de licencia adicionales, agréguelas una por una al repositorio del Servidor de administración de Kaspersky Security Center Cloud Console.

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

   Elija un método para desplegar la clave de licencia (o las claves de licencia) a los dispositivos que desee proteger:

   - Despliegue automático

     > Si usa aplicaciones administradas diferentes y necesita desplegar un código de activación específico para cada una de ellas, elija otra manera de desplegar esos códigos de activación.

     Kaspersky Security Center 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 la clave de licencia automáticamente a los dispositivos administrados** para las tres. 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 y se debe desplegar una clave de licencia para esa aplicación. La aplicación determina, por ejemplo, que dos de las claves de licencia del repositorio se pueden desplegar para la aplicación administrada en el dispositivo: una clave de licencia llamada *Clave_1* y una clave de licencia llamada *Clave_2*. Se despliega una de estas claves de licencia para la aplicación administrada. No es posible predecir cuál es la clave de licencia desplegada porque el despliegue automático de claves de licencia no es un proceso con el que el administrador pueda interactuar.

     Cada vez que se despliega una clave de licencia, se realiza un nuevo conteo del número de instalaciones para los que se la ha utilizado. Asegúrese siempre de que la cantidad de aplicaciones para las que se despliega una clave de licencia no supere el límite definido para la licencia. Si la cantidad de dispositivos excede el límite de la licencia, a todos los dispositivos que no estaban cubiertos por la licencia se les asignará el estado *Crítico*.

     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 "Agregar clave de licencia" para una aplicación administrada, seleccione la clave que quiera desplegar a los dispositivos y, luego, elija los dispositivos utilizando cualquier método que le resulte conveniente (por ejemplo, elija 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 se han activado las aplicaciones de Kaspersky administradas**

   Para verificar que las claves de licencia se hayan desplegado correctamente, consulte la lista de claves de licencia utilizadas para una aplicación.

6. **Configurar eventos relacionados con la caducidad de las licencias**

   Configure los eventos necesarios para recibir una notificación cuando las claves de licencia estén a punto de caducar o ya se hayan utilizado al máximo:

   - Eventos del Servidor de administración: nivel Crítico
   - Eventos del Servidor de administración: nivel Error funcional
   - Eventos del Servidor de administración: nivel Advertencia
   - Eventos del Servidor de administración: nivel Información

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. Está pensado para que el usuario se familiarice con las funciones de Kaspersky Security Center Cloud Console. En este modo, se pueden realizar actividades dentro de un espacio de trabajo con un período de vigencia limitado a treinta días. El modo de prueba se activa automáticamente cuando se crea un espacio de trabajo de prueba. Mientras esté trabajando en este modo, tendrá acceso a las mismas funciones que tendría con la licencia estándar de Kaspersky Endpoint Security for Business Advanced.

En Kaspersky Security Center Cloud Console, no se necesita asignar una licencia para el Servidor de administración, pues las funciones para las que se requiere una licencia especial no son compatibles. Si desea utilizar Kaspersky Security Center Cloud Console en modo de prueba, cree su primer espacio de trabajo y obtendrá automáticamente una licencia de prueba.

No es posible pasar del modo de prueba al modo comercial. Los espacios de trabajo de prueba se eliminan automáticamente, junto con todo su contenido, cuando se llega al límite de treinta días.

En el modo de prueba, la funcionalidad de Kaspersky Security Center Cloud Console está sujeta a las siguientes restricciones:

- No se puede crear una jerarquía de servidores de administración. No se pueden crear servidores de administración virtuales.
- La sección **Licencias** está disponible en modo de solo lectura. No está permitido agregar o quitar claves de licencia ni realizar ningún otro tipo de operación en esta sección.
- No se pueden crear paquetes de instalación personalizados.
- No se pueden crear roles personalizados para los usuarios.
- La función Brote de virus no está disponible. Los eventos Brote de virus no se almacenan y no se envían notificaciones.

- El repositorio **Objetos eliminados** no está disponible.
- No se puede habilitar la adición de eventos agrupados en lotes (eventos que se publican en grandes cantidades) a la base de datos.
- No se admite la migración de servidores de administración del modo local al modo Cloud Console.
- La información estadística de KSN que se recibe de los componentes del Servidor de administración, como el Agente de red o el Servidor de administración, no se envía a Kaspersky.

También se imponen algunos límites a la creación de ciertos objetos de la aplicación (consulte la siguiente tabla). Si supera un límite al intentar crear uno de estos objetos, no se le permitirá crear el objeto en cuestión y verá un mensaje de error sobre el límite.

Limitaciones para crear objetos de Kaspersky Security Center Cloud Console en el modo de prueba

Tipo de limitación	Valor
Directivas	8
Tareas	17
Claves de licencia	1
Paquetes de instalación	5
Selecciones de dispositivos (excluidas las instancias preestablecidas)	5
Selecciones de eventos (excluidas las instancias preestablecidas)	5
Reglas de movimiento de dispositivos	3
Plantillas de informes de un mismo tipo	10
Grupos de seguridad internos	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. Una vez que elija una solución, Kaspersky Security Center Cloud Console lo llevará al sitio web de Kaspersky, a una página web con más información sobre el producto. 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:

  - **Endpoints**: estaciones de trabajo utilizadas por los empleados, máquinas físicas y virtuales, sistemas integrados
  - **Servidores**: servidores físicos y virtuales
  - **Nube**: entornos de nube pública, privada o híbrida; servicios en la nube
  - **Red**: red de área local, infraestructura de TI
  - **Servicios**: servicios relacionados con la seguridad proporcionados por Kaspersky

Para buscar y comprar una solución empresarial de Kaspersky:

1. En el menú principal, vaya a **Marketplace**.

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

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

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

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

Licencias y cantidad mínima de dispositivos para cada licencia

Si desea utilizar Kaspersky Security Center Cloud Console en modo comercial, debe comprar una licencia antes de crear su primer espacio de trabajo. En la siguiente tabla, se enumeran las licencias que puede adquirir y la cantidad mínima de dispositivos que exige cada licencia (el mínimo aplica aunque quiera proteger menos dispositivos):

Licencias que permiten utilizar Kaspersky Security Center Cloud Console

Licencia	Cantidad mínima de dispositivos (aunque quiera proteger menor dispositivos)
Kaspersky Endpoint Security for Business Select	Para licencias comerciales: 300

	Para licencias comerciales (obtenidas por suscripción): 100
Kaspersky Endpoint Security for Business Advanced	Para licencias comerciales: 300 Para licencias comerciales (obtenidas por suscripción): 100
Kaspersky Total Security for Business	300
Kaspersky Endpoint Detection and Response Optimum	Para licencias comerciales: 300 Para licencias comerciales (obtenidas por suscripción): 100
Kaspersky Endpoint Detection and Response Expert	50
Kaspersky Hybrid Cloud Security, escritorios	Para licencias comerciales: 300 Para licencias comerciales (obtenidas por 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 (obtenidas por 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 (obtenidas por suscripción): 100 usuarios Cada licencia de usuario puede aplicarse a 1 PC/Mac y a 2 dispositivos móviles.
Kaspersky Next EDR Optimum	Para licencias comerciales: 300 usuarios Para licencias comerciales (obtenidas por suscripción): 100 usuarios Cada licencia de usuario puede aplicarse a 1 PC/Mac y a 2 dispositivos móviles.
Kaspersky Next Complete Security	Para licencias comerciales: 300 usuarios Para licencias comerciales (obtenidas por suscripción): 100 usuarios Cada licencia de usuario puede aplicarse a 1 PC/Mac y a 2 dispositivos móviles.
Kaspersky Next EDR Expert	250 usuarios Cada licencia de usuario puede aplicarse a 1 PC/Mac y a 2 dispositivos móviles.
Kaspersky Next XDR Expert	250 usuarios Cada licencia de usuario puede aplicarse a 1 PC/Mac y a 2 dispositivos móviles.

Si desea proteger más de 10 000 dispositivos, debe enviar una solicitud al Servicio de 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 le permite obtener información sobre los eventos que se registran cuando las aplicaciones de Kaspersky instaladas en los dispositivos cliente superan algún límite de sus licencias.

El nivel de importancia de estos eventos cuando se supera un límite de licencia se define según las siguientes reglas:

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

Métodos para distribuir los códigos de activación a los dispositivos administrados

Cada aplicación de Kaspersky instalada en un dispositivo administrado debe contar con una licencia. Para agregar estas licencias, se debe aplicar un código de activación en cada aplicación. Los códigos de activación son la única vía válida para agregar una licencia a las aplicaciones administradas; no es posible utilizar archivos de clave para este fin. Para desplegar un código de activación, puede recurrir a los siguientes métodos:

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

Las aplicaciones de Kaspersky pueden usar más de una clave de licencia al mismo tiempo. Kaspersky Endpoint Security para Windows, por ejemplo, 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.

Agregar una clave de licencia del Servidor de administración

Para agregar una clave de licencia del Servidor de administración:

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

   Se abrirá la ventana de propiedades del Servidor de administración, 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 agregar una clave de licencia activa.
   - **Clave de licencia de reserva**, si desea agregar una clave de licencia de reserva.

Puede agregar una clave de licencia de reserva solo si ya se agregó 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 agregar una nueva clave de licencia; para ello, haga clic en el botón **Agregar nueva clave de licencia** y luego ingrese la clave de licencia en el panel derecho que se abre.

4. Haga clic en el botón **Aceptar**.

Se cierra la ventana, se agrega 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

Si agrega una clave de licencia a través de Kaspersky Security Center Cloud Console, las propiedades de la misma quedarán almacenadas 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 **Agregar**.

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 la aplicación**. Con la tarea, puede distribuir claves a un grupo de dispositivos específico. Durante la distribución de una clave de licencia mediante una tarea, no se tiene en cuenta el límite de obtención de licencias en el número de dispositivos. Use la distribución automática de claves para detener la distribución de una clave de licencia automáticamente cuando se alcance el límite de obtención de licencias.

Si habilita la opción Distribución automática de una clave de licencia, no cree una tarea de **Activación de la aplicación** para distribuir la clave a los dispositivos cliente. De lo contrario, la carga en el Servidor de administración aumentará debido a la frecuencia de la sincronización.

Antes de realizar la distribución, agregue la clave de licencia al repositorio del Servidor de administración.

*Para distribuir una clave de licencia a los dispositivos cliente con la tarea de **Activación de la aplicación**:*

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el **Asistente para crear nueva tarea**. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. En la lista desplegable **Aplicación**, seleccione la aplicación para la que desee agregar una clave de licencia.
4. En la lista **Tipo de tarea**, seleccione la tarea de **Activación de la aplicación**.
5. En el campo **Nombre de la tarea**, ingrese el nombre de la tarea nueva.
6. Seleccione los dispositivos a los que se asignará la tarea.
7. En el paso **Seleccionar una clave de licencia** del asistente, haga clic en el vínculo **Agregar clave** para agregar la clave de licencia.
8. En el panel para agregar claves, agregue la clave de licencia mediante una de las siguientes opciones:

   Debe agregar la clave de licencia solo si no la agregó al repositorio del Servidor de administración antes de crear la tarea de **Activación de la aplicación**.

   - Seleccione la opción **Escribir código de activación** para ingresar un código de activación y luego haga lo siguiente:

     a. Especifique el código de activación y haga clic en el botón **Enviar**.

        La información sobre la clave de licencia aparece en el panel para agregar claves.

     b. Haga clic en el botón **Guardar**.

        Si desea distribuir la clave de licencia a los dispositivos administrados de forma automática, habilite la opción **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.

        Se cerrará el panel para agregar claves.

   - Seleccione la opción **Agregar archivo de clave** para agregar un archivo de clave y luego haga lo siguiente:

     a. Haga clic en el botón **Seleccionar archivo de clave**.

     b. En la ventana que se abre, seleccione un archivo de clave y haga clic en el botón **Abrir**.

        La información sobre la clave de licencia aparecerá en el panel para agregar claves de licencia.

     c. Haga clic en el botón **Guardar**.

Si desea distribuir la clave de licencia a los dispositivos administrados de forma automática, habilite la opción **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.

Se cerrará el panel para agregar claves.

9. Seleccione la clave de licencia desde la tabla de claves.

10. En el paso **Información de licencia** del asistente, desmarque la casilla **Usar como clave de reserva** predeterminada si desea reemplazar la clave de licencia activa.

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

    Si desea obtener más información sobre las cuestiones que pueden surgir al agregar una clave de licencia a Kaspersky Security Center y cómo resolverlas, consulte la Base de conocimientos de Kaspersky Security Center.

11. En el paso **Finalizar la creación de la tarea** del asistente, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** para modificar la configuración predeterminada de la tarea.

    Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificarla más adelante.

12. Haga clic en el botón **Finalizar**.

    El asistente creará la tarea. Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá automáticamente la ventana de propiedades de la tarea. En esta ventana, puede definir la configuración general de la tarea y, si es necesario, cambiar los ajustes establecidos durante la creación de la tarea.

    También puede abrir la ventana de propiedades de la tarea haciendo clic en el nombre de la tarea creada en la lista de tareas.

    La tarea se creará, configurará y se mostrará en la lista de tareas.

13. Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

    También puede programar el inicio de la tarea en la pestaña **Programación**, en la ventana de propiedades de la tarea.

    Para obtener una descripción detallada de la configuración de inicio programado, consulte la configuración general de la tarea.

Cuando se complete la tarea, la clave de licencia se desplegará a los dispositivos seleccionados.

Distribución automática de una clave de licencia

Kaspersky Security Center Cloud Console permite que las claves de licencia almacenadas el repositorio de claves de licencia del Servidor de administración se distribuyan en forma automática a los dispositivos administrados.

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, ponga el interruptor en la posición **Distribuir la clave de licencia automáticamente a los dispositivos administrados**.

4. Haga clic en el botón **Guardar**.

La clave de licencia se distribuirá automáticamente a todos los dispositivos compatibles.

La distribución de claves de licencia se realiza a través del Agente de red. No se crean tareas de distribución de clave de licencia para la aplicación.

Durante la distribución automática de una clave de licencia, se tiene en cuenta el límite de obtención de licencias en el número de dispositivos. Este límite está definido en las propiedades de la clave de licencia. Cuando se llega al límite de dispositivos, el proceso de distribución se detiene automáticamente y la clave de licencia no se transfiere a más dispositivos.

Tenga en cuenta que una clave de licencia distribuida automáticamente podría no aparecer en el repositorio del Servidor de administración virtual en los siguientes casos:

- La clave de licencia no es válida para la aplicación.
- El Servidor de administración virtual no tiene ningún dispositivo administrado.
- La clave de licencia ya ha sido utilizada para dispositivos administrados asociados a otro Servidor de administración virtual y se ha alcanzado el límite a la cantidad de dispositivos.

Si habilita la opción **Distribuir la clave de licencia automáticamente a los dispositivos administrados** para una clave de licencia de suscripción a fin de activar cualquier aplicación en un dispositivo administrado y, al mismo tiempo, tiene activa una clave de licencia de prueba, la clave de licencia de prueba se reemplazará automáticamente ocho días antes de su caducidad por la clave de licencia de suscripción.

Ver información sobre las claves de licencia en uso agregadas al repositorio del Servidor de administración

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

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

Se mostrará una lista con los códigos de activación que se hayan agregado al repositorio del Servidor de administración.

Para ver información detallada sobre una clave de licencia:

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

2. Haga clic en el nombre de la clave de licencia de su interés.

Se abre una ventana con las propiedades de la clave de licencia. En la ventana, puede ver lo siguiente:

- en la pestaña **General**, los datos generales de la clave de licencia;

- en la pestaña **Dispositivos**, la lista de dispositivos cliente en los que la clave de licencia se utilizó para activar la aplicación de Kaspersky instalada.

Ver información sobre las claves de licencia utilizadas para una aplicación de Kaspersky

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 **Descubrimiento y despliegue** → **Dispositivos no asignados**.

2. Haga clic en el nombre del dispositivo pertinente.

3. En la ventana que se abre, que contendrá las propiedades del dispositivo, vaya a la sección **Aplicaciones**.

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

5. En la ventana de las 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.

Eliminar 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 ( ) ubicado junto al 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 agregó una clave de licencia de reserva, al eliminar la clave de licencia activa, la clave de reserva se convertirá automáticamente en la clave de licencia activa.

Después de que se haya eliminado la clave de licencia activa del Servidor de administración, las funciones Administración de vulnerabilidades y parches y Administración de dispositivos móviles no están disponibles. Puede volver a agregar una clave de licencia eliminada o agregar una clave de licencia nueva.

Eliminar una clave de licencia del repositorio

Puede eliminar una clave de licencia del repositorio del Servidor de administración. Tenga en cuenta que los espacios de trabajo de Kaspersky Security Center Cloud Console se eliminan automáticamente luego de noventa días en los siguientes casos:

- cuando se eliminó la última clave de licencia (activa, de reserva o no utilizada) agregada al repositorio manualmente;
- cuando ha caducado la última clave de licencia.

Si su espacio de trabajo se elimina, ya no podrá utilizar Kaspersky Security Center Cloud Console para administrar la protección de su red. También perderá para siempre la información de Kaspersky Security Center Cloud Console. Si lo considera necesario, puede eliminar su espacio de trabajo manualmente. Caso contrario, recomendamos que mantenga al menos una clave de licencia en el repositorio del Servidor de administración.

Si elimina una clave de licencia, pero había agregado una clave de licencia de reserva, la clave de licencia de reserva se convertirá automáticamente en la clave de licencia activa, en reemplazo de la clave de licencia que supo estar activa y que se eliminó (o que caducó).

Si elimina la clave de licencia activa desplegada en un dispositivo administrado, la aplicación seguirá funcionando en ese dispositivo.

Para eliminar una clave de licencia del repositorio del Servidor de administración:

1. Verifique que el Servidor de administración no esté utilizando la clave de licencia que desea eliminar. Si el Servidor de administración está utilizando ese archivo o código, no lo podrá eliminar. Para realizar la verificación, haga lo siguiente:

   a. En el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al 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 ve la clave de licencia que desea eliminar en esta sección, haga clic en el botón **Eliminar clave de licencia activa** y confirme la operación. El Servidor de administración dejará de utilizar la clave de licencia eliminada, pero no se la borrará del repositorio del Servidor de administración. Si la clave de licencia que desea eliminar no aparece en esta sección, sabrá que no es la que utiliza el Servidor de administración.

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

3. Seleccione la clave de licencia que desee eliminar y haga clic en el botón **Eliminar**.

4. En la ventana que aparece, marque la casilla **Comprendo el riesgo y deseo eliminar la clave de licencia**. Al hacer esto, declara saber que, si elimina su última clave de licencia, su espacio de trabajo se eliminará y ya no podrá controlar sus dispositivos administrados. A continuación, haga clic en el botón **Eliminar**.

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

Puede agregar nuevamente la clave de licencia eliminada o puede agregar una nueva. Si la clave de licencia que eliminó era la última disponible, podrá agregar una nueva en tanto su espacio de trabajo no se haya eliminado. 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 en los que no está activada una aplicación de Kaspersky

Puede ver una lista con los dispositivos en los que una aplicación de Kaspersky se encuentra instalada, pero no está activada (por ejemplo, por no haber una licencia disponible o porque la licencia provista ha caducado).

Para ver los dispositivos en los que 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" vinculada a 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 la tarea se realizó correctamente.

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

   En la columna **Dispositivo o servidor secundario**, se muestran los dispositivos en los que la tarea se realizó correctamente. Los dispositivos en los que la tarea no se haya completado correctamente serán aquellos en los que, por falta de licencia, la aplicación no se encuentre 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. Antes de revocar el EULA, deberá eliminar la aplicación y los paquetes de instalación a los que el contrato esté asociado. Deberá borrar los paquetes de instalación del Servidor de administración y de 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, elija la sección **Contratos de licencia de usuario final**.

   Se muestra una lista de los EULA aceptados al crear paquetes de instalación o al instalar actualizaciones sin interrupciones.

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 puede revocarse 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.
   - Una lista de los objetos (paquetes de instalación, actualizaciones sin interrupciones) 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**.

   En caso de que el EULA seleccionado se pueda revocar solo desinstalando la aplicación, o bien si este EULA se puede revocar solo en el Servidor de administración principal, se mostrará una notificación sobre esta restricción en lugar del botón **Revocar el Contrato de licencia**.

   > De existir algún objeto que impida revocar el EULA (algún paquete de instalación con su respectiva tarea), verá una notificación. No podrá revocar el contrato hasta que haya eliminado el objeto problemático.

   En la ventana que se abre, se le informa que primero debe desinstalar la aplicación de Kaspersky correspondiente al EULA.
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).

> Noventa días después de que caduque su última clave de licencia, Kaspersky Security Center Cloud Console eliminará automáticamente su espacio de trabajo. Una vez que esto ocurra, no podrá utilizar Kaspersky Security Center Cloud Console para administrar la protección de su red. También perderá para siempre la información de Kaspersky Security Center Cloud Console. Recomendamos que renueve sus claves de licencia antiguas o que agregue claves de licencia nuevas al repositorio del Servidor de administración para no perder su espacio de trabajo.

Para ver una notificación sobre una licencia que ha caducado o que está próxima a caducar:

1. Realice alguna de las siguientes acciones:

   - En el menú principal, vaya a **Operaciones** → **Licencias** → **Licencias de Kaspersky**.
   - En el menú principal, vaya a **Supervisión e informes** → **Panel** y haga clic en el vínculo **Ver licencias próximas a caducar** junto a una notificación.

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

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

   > Al hacer clic en el vínculo para renovar una licencia, acepta transferir los siguientes datos a Kaspersky: el id. del software, la versión del software, la localización del software, el id. de la licencia y un atributo que muestra si la licencia fue proporcionada por una empresa asociada. Los datos se necesitan para determinar los términos de renovación de la licencia.

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

   Se renueva la licencia que estaba próxima a caducar.

Cuando una licencia esté próxima a caducar, Kaspersky Security Center Cloud Console mostrará una notificación siguiendo este esquema:

- 30 días antes de la caducidad
- 7 días antes de la caducidad
- 3 días antes de la caducidad
- 24 horas antes de la caducidad
- Cuando la licencia haya caducado

Usar Kaspersky Security Center Cloud Console una vez que caduca la licencia

Si su licencia caduca, puede que Kaspersky le permita seguir utilizando Kaspersky Security Center Cloud Console sin restricciones por hasta noventa días adicionales. Durante este tiempo, el Servidor de administración, el Agente de red y la interfaz web de Kaspersky Security Center Cloud Console seguirán funcionando sin limitaciones. Kaspersky Security Center Cloud Console seguirá enviando estadísticas de KSN a Kaspersky según lo permitan los ajustes de acceso a KSN vigentes. Las aplicaciones administradas tendrán restricciones de funcionamiento (para más información, consulte la documentación de esas aplicaciones).

Noventa días después de la caducidad de la licencia, Kaspersky Security Center Cloud Console eliminará su espacio de trabajo automáticamente. Para conservar el espacio de trabajo, renueve al menos una clave de licencia caducada o agregue una clave de licencia nueva al repositorio.

Terminología de las licencias

En esta sección, se ofrecen definiciones para los conceptos relacionados con las licencias de las aplicaciones de Kaspersky que puede administrar 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 proporcionan los siguientes tipos de licencia:

- *Prueba*

  Una licencia gratuita diseñada para probar la aplicación. Usualmente, una licencia de prueba tiene un plazo de vigencia breve.

  Cuando vence una licencia de prueba, todas las funciones de Kaspersky Security Center Cloud Console se deshabilitan. Para seguir usando la aplicación, se debe adquirir una licencia comercial.

  Puede usar la aplicación con una licencia de prueba solo durante un período de prueba.

- *Comercial*

  Una licencia pagada.

  Cuando caduca una licencia comercial, se deshabilitan las principales características de la aplicación. Para seguir usando Kaspersky Security Center Cloud Console, se debe renovar la licencia comercial. Una vez que caduca una licencia comercial, no puede seguir usando la aplicación y debe eliminarla de su dispositivo.

  Se recomienda renovar la licencia antes de que caduque para garantizar una protección ininterrumpida contra las amenazas a la seguridad.

Acerca del certificado de licencia

Un *certificado de licencia* es un documento que se entrega adjunto a un archivo de clave o código de activación.

El certificado de licencia contiene la siguiente información sobre la licencia proporcionada:

- Clave de licencia o número de pedido
- Información sobre el usuario al que se le ha otorgado la licencia
- Información sobre la aplicación que se puede activar con la licencia otorgada
- Límite al número de unidades con licencia (por ejemplo, el número de dispositivos en los que la licencia otorgada permite usar la aplicación)
- Fecha en que comienza la validez de la licencia
- Fecha de caducidad de la licencia o periodo de vigencia de la licencia
- Tipo de licencia

Acerca de la clave de licencia

La *clave de licencia* es una secuencia de bits que se puede aplicar para activar y utilizar la aplicación de acuerdo con el Contrato de licencia de usuario final. Las claves de licencia son generadas por los especialistas de Kaspersky.

Para agregar una clave de licencia a la aplicación, ingrese 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. Cuando se ingresa esta secuencia, se agrega una clave de licencia que activa Kaspersky Security Center Cloud Console. Le enviaremos un código de activación a la dirección de correo electrónico que nos indique al comprar Kaspersky Security Center Cloud Console o al solicitar la versión de prueba de Kaspersky Security Center Cloud Console.

Para activar la aplicación mediante el código de activación, necesita acceso a Internet para establecer la conexión con los servidores de activación de Kaspersky. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos.

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

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

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

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, número de dispositivos protegidos). Puede registrar su 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 continuar usando Kaspersky Security Center Cloud Console una vez que caduca una suscripción limitada, dicha suscripción se debe renovar. Una suscripción ilimitada se renueva automáticamente si el proveedor de servicios ha recibido a término y por adelantado el pago correspondiente.

Cuando una suscripción limitada caduca, la aplicación puede seguir funcionando por un tiempo adicional, durante un período de gracia. Este período puede aprovecharse para renovar la suscripción. El proveedor de servicios define la disponibilidad y la duración del período de gracia.

Para usar Kaspersky Security Center Cloud Console bajo la modalidad de suscripción, se debe aplicar el código de activación enviado por el proveedor de servicios.

Si necesita aplicar un código de activación diferente a Kaspersky Security Center Cloud Console, deberá cancelar su suscripción o esperar a que caduque.

El conjunto de acciones disponibles para administrar una suscripción puede variar según el proveedor de servicios. Su proveedor de servicios podría no ofrecerle un período de gracia para renovar la suscripción; en tal caso, la aplicación dejará de funcionar.

Los códigos de activación adquiridos por suscripción no se pueden usar para activar versiones anteriores de Kaspersky Security Center Cloud Console.

Cuando la aplicación se utiliza con una suscripción, Kaspersky Security Center Cloud Console intenta contactarse con el servidor de activación en forma periódica y automática. Estos intentos de comunicación se repiten hasta que la suscripción caduca. Si los servidores DNS configurados en el sistema no permiten acceder al servidor de Kaspersky, la aplicación utiliza servidores DNS públicos. Si necesita renovar su suscripción, puede hacerlo en el sitio web de su proveedor de servicios.

Provisión de datos

Kaspersky Security Center Cloud Console permite que, mediante las funciones de las aplicaciones administradas, el usuario identifique y controle los dispositivos conectados a Kaspersky Security Center Cloud Console, así como a los propietarios de dichos dispositivos.

Métodos de provisión de datos:

1. El usuario ingresa información en la interfaz de Kaspersky Security Center Cloud Console.
2. El Agente de red recibe datos del 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. Para ver la lista de datos que trata o procesa cada aplicación de Kaspersky administrada, consulte los documentos de ayuda de esas aplicaciones.
4. Los datos se transfieren desde los servidores de administración secundarios que operan en una infraestructura local.

Kaspersky Security Center Cloud Console elimina automáticamente los espacios de trabajo treinta días después de que caduca la licencia de prueba o noventa días después de que caduca 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 e incidentes es de 360 días. Después de este período, 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 transmitidos a los servidores de Kaspersky

Datos que se transmiten durante la activación

Al usar el código de activación para activar el software, el usuario acepta proporcionar periódicamente la siguiente información a Kaspersky a fin de que se verifique la legitimidad del uso del software:

- Código de activación
- Identificador de activación único correspondiente a la licencia utilizada

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

Datos que se transmiten durante una actualización

Tras recibir actualizaciones de los servidores de actualizaciones del titular de los derechos, el usuario acepta proporcionar periódicamente la siguiente información a Kaspersky para que se pueda mejorar el mecanismo de actualización:

- Id. del software recibido de la licencia

- Versión completa del software
- Id. de la licencia del software
- Id. de instalación del 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 la cantidad de dispositivos en los que están instaladas esas aplicaciones.
- Cantidad de dispositivos con aplicaciones de seguridad de Kaspersky instaladas que se han conectado 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 autentificación en el espacio de trabajo.
- Detalles de la licencia que se esté utilizando (tipo de licencia, límite de dispositivos en los que la licencia puede utilizarse, cantidad de dispositivos conectados, fecha de caducidad de la licencia utilizada anteriormente).

Datos que se transfieren al abrir los vínculos de la interfaz de Kaspersky Security Center Cloud Console

Al hacer clic en un vínculo de la Consola de administración o de Kaspersky Security Center Cloud Console, el usuario acepta que se transfieran automáticamente los siguientes datos:

- Localización de Kaspersky Security Center Cloud Console
- Id. de la 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

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

a. Especificaciones técnicas del dispositivo y de sus componentes que se necesitan para identificar el dispositivo y que se reciben al realizar un sondeo de red:

- Sondeo de Active Directory:

  Dispositivos de Active Directory: nombre distintivo del dispositivo; nombre de dominio de Windows enviado por el controlador de dominio; nombre del dispositivo en el entorno de Windows; nombre de dominio NetBIOS; dominio DNS y nombre DNS del dispositivo; cuenta de administrador de cuentas de seguridad (SAM) (nombre para iniciar sesión en el sistema utilizado por motivos de compatibilidad con clientes y servidores con 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; e identificador único global (GUID) y GUID principal del dispositivo.

  Cuando se realiza un sondeo de la red de Active Directory, también se tratan o procesan los siguientes tipos de datos con el fin de mostrar información sobre la infraestructura administrada y permitir que el usuario utilice esa información durante, por ejemplo, el despliegue de la protección:

- Unidades organizativas de Active Directory: nombre distintivo de la unidad organizativa; nombre distintivo del dominio; GUID y GUID principal 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 en el que trabaja el usuario; nombre distintivo del usuario designado como administrador del usuario; nombre completo del usuario; cuenta SAM; dirección de correo electrónico; dirección de correo electrónico alternativa; 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 (SID) del usuario (valor binario único que identifica al usuario como entidad de seguridad); nombre principal de usuario (UPN). Este último dato es un tipo de nombre que el usuario puede usar para iniciar sesión. El UPN está basado en el estándar de Internet RFC 822 y se asemeja a los nombres que se usan en Internet. Es más breve y más fácil de recordar que los nombres distintivos. Por convención, el UPN se corresponde con el nombre de correo electrónico del usuario.

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

b. Sondeo del dominio de Samba:

Dispositivos Samba: nombre distintivo del dispositivo; nombre de dominio enviado por el controlador de dominio; nombre NetBIOS del dispositivo; nombre NetBIOS del dominio; dominio DNS y nombre DNS del dispositivo; cuenta de administrador de cuentas de seguridad (SAM); 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 principal del dispositivo.

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

- Dominio de Samba: nombre de dominio enviado por el 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 en el que trabaja el usuario; nombre distintivo de otro usuario que actúa como responsable del usuario; nombre completo del usuario; cuenta SAM; dirección de correo electrónico; dirección de correo electrónico alternativa; número de teléfono principal; número de teléfono alternativo; número de teléfono móvil; nombre del cargo del usuario; nombres distintivos de

los grupos a los que pertenece el usuario; identificador único global (GUID) del usuario; identificador de seguridad (SID) del usuario (valor binario único utilizado para identificar al usuario como entidad de seguridad); nombre principal del usuario (UPN): nombre de usuario al estilo de Internet para un usuario basado en el estándar de Internet RFC 822. Es más breve y más fácil de recordar que los nombres distintivos. Por convención, el UPN se corresponde con el nombre de correo electrónico del usuario.

- Grupos de Samba: nombre distintivo del grupo; dirección de correo electrónico; nombre distintivo del dominio; cuenta SAM; nombres distintivos de otros grupos a los que pertenece el grupo; grupo SID; GUID del 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 instalado en el dispositivo
- Versión del sistema operativo instalado el dispositivo
- Hora en que la información sobre el dispositivo se actualizó por última vez
- Hora en que el dispositivo estuvo visible en la red por última vez

d. Sondeo de intervalos IP:

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

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 nombre y la descripción del dispositivo son introducidos por el usuario en la interfaz de Kaspersky Security Center Cloud Console.

a. Especificaciones técnicas del dispositivo administrado y de sus componentes necesarias para identificar el dispositivo:

- Nombre del dispositivo (este dato se genera sobre la base del nombre NetBIOS y puede modificarse en forma manual) y descripción del dispositivo (este dato se ingresa en forma manual)

- Nombre de dominio de Windows y tipo de dominio (dominio de Windows NT o 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 instalado en el dispositivo
- Indicación de si el dispositivo es una máquina virtual y tipo de hipervisor
- Indicación de si el dispositivo es una máquina virtual dinámica que forma parte de una infraestructura de escritorios virtuales (VDI)
- Identificador único global del dispositivo
- Id. de la instancia del Agente de red
- Id. de instalación del Agente de red
- Id. permanente del Agente de red

b. Otras especificaciones de los dispositivos administrados y de sus componentes que se necesitan para auditar los dispositivos administrados y para determinar si ciertos parches y actualizaciones deben aplicarse:

- Estado del Agente de Windows Update (WUA)
- Arquitectura del sistema operativo
- Proveedor del sistema operativo
- Número de compilación del sistema operativo
- Id. de versión del sistema operativo
- Carpeta de ubicación del sistema operativo
- Si el dispositivo es una máquina virtual, el tipo de máquina virtual
- Tiempo de espera para respuestas del dispositivo
- Indicación de si el Agente de red se ejecuta en modo independiente

c. Información detallada sobre actividades que suceden en los dispositivos administrados:

- Fecha y hora de la última actualización
- Fecha y hora en que el dispositivo estuvo visible en la red por última vez
- Estado de espera de reinicio ("Se debe reiniciar el dispositivo.")
- Hora en que se encendió el dispositivo

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

e. Estadísticas de funcionamiento del punto de distribución (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
- Cantidad de sincronizaciones con el Servidor de administración
- Fecha y hora en que el dispositivo se sincronizó por última vez con el Servidor de administración
- Cantidad de archivos transferidos y tamaño total de esos archivos
- Cantidad de archivos descargados por los clientes y tamaño total de esos archivos
- Volumen de datos descargado por los clientes a través del protocolo TCP (protocolo de control de transmisión)
- Volumen de datos enviado a los clientes por multidifusión
- Volumen de datos descargado por los clientes mediante multidifusión
- Cantidad de distribuciones multidifusión
- Volumen total de las distribuciones multidifusión
- Cantidad de sincronizaciones con los 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. Encontrará la lista de datos completa 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. Aplicaciones de Kaspersky administradas y componentes de Kaspersky Security Center Cloud Console instalados en el dispositivo

   b. Propiedades 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
      - Cantidad de amenazas detectadas
      - Cantidad de objetos que no se pudieron desinfectar
      - Tareas para la aplicación de seguridad de Kaspersky
      - Disponibilidad y estado de los componentes de la aplicación
      - Versión de las bases de datos antivirus y hora en que se actualizaron por última vez
      - Detalles de configuración de la aplicación de Kaspersky
      - Información sobre las claves de licencia activas
      - Información sobre las claves de licencia de reserva
      - Fecha de instalación de la aplicación
      - Id. de instalación de la aplicación

   c. Estadísticas sobre el funcionamiento de la aplicación: eventos relacionados con los cambios en el estado de los componentes de la aplicación de Kaspersky instalada en el dispositivo administrado y eventos relacionados con la ejecución 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 aplicables en la aplicación de Kaspersky:

      - Nombre, versión e idioma de la aplicación
      - Nombre interno de la aplicación
      - Nombre y versión de la aplicación en la clave del Registro
      - Carpeta de instalación de la aplicación

- Versión del parche
- Lista de parches automáticos instalados en la aplicación
- Indicación de si la aplicación es compatible con Kaspersky Security Center Cloud Console
- Indicación de si la aplicación se encuentra instalada en un clúster

g. Detalles de los errores de cifrado de datos registrados en los dispositivos: id. del error, hora en que ocurrió, tipo de operación (cifrado o descifrado), descripción del error, ruta de 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 de las aplicaciones de Kaspersky administradas.

   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 del usuario del dispositivo

   c. Nombre del administrador que se conectó 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. Ruta al archivo en el dispositivo y nombre del archivo

   g. Nombre de la aplicación y parámetros de línea de comandos que se usaron para iniciarla

   h. Nombre del parche, nombre del archivo del parche, identificador del parche, nivel de la vulnerabilidad corregida por el parche, 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 con la cual se publicó el evento

   m. Indicación de si el dispositivo cambió al modo independiente y motivo de ese 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. Cantidad de espacio libre en el disco del dispositivo

   p. Indicación de si la aplicación de Kaspersky está operando en modo de funcionalidad limitada e identificadores de los ámbitos funcionales

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

r. Descripción del error que ocurrió cuando la aplicación de Kaspersky o alguno de sus componentes realizó la operación

5. Ajustes de los componentes de Kaspersky Security Center Cloud Console y de las aplicaciones de Kaspersky administradas que están presentes en las directivas y en los perfiles de directivas.

   El usuario ingresa información en la interfaz de Kaspersky Security Center Cloud Console.

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

   El usuario ingresa información en la interfaz de Kaspersky Security Center Cloud Console.

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

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

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

      - Id. de la aplicación o del parche
      - Id. de la aplicación principal (en el caso de los parches)
      - Nombre y versión de la aplicación o del parche
      - Indicación de si la aplicación o el parche son un archivo .msi de Windows Installer
      - Proveedor de la aplicación o del parche
      - Identificador del idioma de localización
      - Fecha de instalación de la aplicación o del parche
      - Ruta de instalación de la aplicación
      - Sitio web del servicio de soporte técnico del proveedor de la aplicación o del parche
      - Número de teléfono del servicio de soporte técnico
      - Identificador de la instancia de aplicación instalada
      - Comentario
      - Clave de desinstalación
      - Clave de instalación en modo silencioso
      - Clasificación del parche
      - Dirección web para obtener información adicional sobre el parche
      - Clave del Registro de la aplicación
      - Número de compilación de la 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 madre, CPU, RAM, dispositivo de almacenamiento masivo, adaptador de video, tarjeta de sonido, controlador de interfaz de red, monitor, unidad de disco óptico)
- Nombre del dispositivo
- Descripción
- Proveedor
- Número de serie
- Revisión
- Información sobre el controlador: desarrollador, versión, descripción, fecha de lanzamiento
- Información sobre la BIOS: desarrollador, versión, número de serie, fecha de lanzamiento
- Chipset
- Velocidad de reloj
- Cantidad de núcleos de la CPU
- Cantidad de subprocesos de la CPU
- Plataforma de la CPU
- Velocidad de rotación del dispositivo de almacenamiento
- RAM: tipo, número de pieza
- Memoria de video
- Códec de la tarjeta de sonido

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

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

- Id. del 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 bloquean la vulnerabilidad (Protección contra archivos peligrosos, Detección de comportamiento, Protección contra amenazas web, Protección contra amenazas de correo, Prevención de intrusiones en el host, ZETA Shield)
- Ruta al archivo objeto en el que se detectó la vulnerabilidad
- Hora en que se detectó la vulnerabilidad
- Identificadores de los artículos de la Base de conocimientos de la descripción de vulnerabilidad
- Identificadores de los boletines de seguridad de la descripción de vulnerabilidad
- Lista de actualizaciones disponibles para la vulnerabilidad
- Indicación de si existe un exploit para la vulnerabilidad
- Indicación de si existe malware para la vulnerabilidad

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

- Nombre y versión de la aplicación
- Proveedor
- Idioma de localización de la aplicación
- Sistema operativo
- Lista de parches en orden de instalación
- Versión original de la aplicación a la que se aplica el parche
- Versión de la aplicación después de la instalación del parche
- Identificador del parche
- Número de compilación
- Marcas de instalación
- Contratos de licencia del parche

- Indicación de si el parche es un requisito previo para instalar otros parches
- Lista de las aplicaciones que deben estar instaladas y sus actualizaciones
- Fuentes de información sobre el parche
- Información adicional sobre el parche (direcciones de páginas web)
- Dirección web para descargar el parche, el nombre de archivo, la versión, la revisión y el hash 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 (Bajo, Medio, Alto, Crítico) según el boletín del Centro de respuestas de seguridad de Microsoft (MSRC)
- Identificadores de los boletines del MSRC relacionados con la actualización
- Identificadores de los artículos de la Base de conocimientos del MSRC
- Nombre de la actualización (encabezado)
- Descripción de la actualización
- Indicación de si el instalador de la actualización es interactivo
- Marcas de instalación
- Clasificación de la actualización ("Actualizaciones críticas", "Actualizaciones de definiciones", "Controladores", "Paquetes de características", "Actualizaciones de seguridad", "Service Packs", "Herramientas", "Paquetes acumulativos de actualizaciones", "Actualizaciones", "Upgrades")
- Información sobre la aplicación a la que se aplica la actualización
- Identificador del Contrato de licencia de usuario final (EULA)
- Texto del EULA
- Indicación de si se debe aceptar el EULA para instalar la actualización
- Información sobre las actualizaciones asociadas (id. y número de revisión)
- Id. de la actualización (identidad de actualización global de Microsoft Windows)
- Identificadores de las actualizaciones reemplazadas
- Indicación de si la actualización está oculta
- Indicación de si la actualización es obligatoria
- Estado de instalación de la actualización ("No se aplica", "Instalación no asignada", "Asignada", "Instalándose", "Instalada", "Error", "Se debe reiniciar el dispositivo", "Instalación no asignada (nueva versión)")

- Identificadores CVE de la actualización
- Empresa que publicó la actualización o, en su defecto, el valor "Falta 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 (esta información puede estar asociada a la información del registro de aplicaciones). Encontrará una lista con todos los datos en la sección en la que se describen los datos para 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 almacenados en Copia de seguridad. Encontrará una lista con todos los datos en la sección en la que se describen los datos para 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 archivos solicitada por los especialistas de Kaspersky para realizar un análisis detallado. Encontrará una lista con todos los datos en la sección en la que se describen los datos para 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 del Control de anomalías adaptativo. Encontrará una lista con todos los datos en la sección en la que se describen los datos para 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 para copias de información impresas y buses de conexión) que se han instalado en el dispositivo administrado o que se han conectado a este y que fueron detectados por la función Control de dispositivos. Encontrará una lista con todos los datos en la sección en la que se describen los datos para 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 ingresa 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 del 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 agregó el comentario
  - Usuario que agregó el comentario
  - Texto del comentario
- Alerta de registro de cambios:
  - Fecha y hora del cambio
  - Usuario que realizó el cambio
  - Cambiar descripción

14. Datos sobre problemas de seguridad:

- Fecha y hora del primer evento del problema de seguridad
- Fecha y hora del último evento del problema de seguridad
- Nombre del problema de seguridad (el usuario lo ingresa 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, positivo verdadero, baja prioridad, fusión)
- Comentario sobre el problema de seguridad:
  - Fecha y hora en que se agregó el comentario

- Usuario que agregó el comentario
- Texto del comentario

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

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

    La aplicación administrada transfiere los datos indicados a continuación del dispositivo al Servidor de administración a través del Agente de red. La descripción de la unidad es introducida por el usuario en la interfaz de Kaspersky Security Center Cloud Console:

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

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

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

       Encontrará una lista con todos los datos en la sección en la que se describen los datos para dispositivos administrados a través de la aplicación correspondiente.

16. Detalles de los códigos de activación ingresados.

    El usuario ingresa información en la interfaz de Kaspersky Security Center Cloud Console.

17. Cuentas de usuario.

El usuario ingresa los datos que se enumeran 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 que se necesitan para autenticar al usuario con 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 de token que contiene el SID de usuario
    - Nombre del campo de token que contiene la matriz de SID de los grupos del usuario

    El usuario ingresa información 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 ingresa información 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 revisiones de los objetos de administración: Servidor de administración, grupo de administración, directiva, tarea, usuario o grupo de seguridad, paquete de instalación.

    a. El usuario ingresa los datos que se enumeran a continuación en la interfaz de Kaspersky Security Center Cloud Console:

    - Servidor de administración

    - Grupo de administración

    - Directiva

    - Tarea

    - Usuario o 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 ingresa información en la interfaz de Kaspersky Security Center Cloud Console.

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

    El usuario ingresa información en la interfaz de Kaspersky Security Center Cloud Console.

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

    a. Información sobre las aplicaciones de Kaspersky administradas que el usuario utiliza: id. de la aplicación y número de versión completo.

    b. Localización elegida por el usuario para la interfaz de Kaspersky Security Center Cloud Console.

    c. Información sobre la activación del software en el dispositivo: id. de la licencia del software; período 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 de software; estado actual de la suscripción de software; motivo del estado actual o del cambio de estado de la

suscripción de software; id. del artículo de la lista de precios a través de la cual se adquirió la licencia del software.

d. Información sobre el acuerdo legal aceptado por el usuario al utilizar el software: tipo de acuerdo legal; versión del acuerdo legal; marca que indica si el usuario aceptó las condiciones del acuerdo legal.

e. Información sobre las novedades recibidas del titular de los derechos: id. de la novedad, hora de recepción de la novedad, estado de recepción de la novedad.

El usuario ingresa información en la interfaz de Kaspersky Security Center Cloud Console.

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

    El usuario ingresa los datos que se enumeran 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 del aspecto del panel de supervisión

    d. Información sobre el estado de la notificación: Leída / No leída

    e. Estado de las columnas en las hojas de cálculo: Mostrar/Ocultar

    f. Progreso del tutorial

25. Datos recibidos al utilizar 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 registro, resultados de la ejecución de scripts de diagnóstico enviados por Soporte técnico.

26. Datos que el usuario ingresa 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 por correo electrónico

    c. Etiquetas para dispositivos y reglas de etiquetado

    d. Etiquetas para aplicaciones

    e. Categorías de aplicaciones creadas por el usuario

    f. Nombre del rol al asignarle un rol a un usuario

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

    h. Configuración de informes y selecciones

    i. Cualquier otro dato ingresado por el usuario

27. Datos recibidos de un Servidor de administración secundario desplegado en una infraestructura local.

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

Cuando un Servidor de administración de Kaspersky Security Center que se encuentra desplegado en una infraestructura local se conecta como Servidor de administración secundario de Kaspersky Security Center Cloud Console, Kaspersky Security Center Cloud Console trata los siguientes tipos de datos de ese Servidor de administración secundario:

a. Información sobre los dispositivos conectados a la red de la organización, recibida mediante el análisis de intervalos IP o como resultado del descubrimiento de dispositivos en la red de Active Directory o la red de Windows

b. Información sobre las unidades organizativas, los dominios, los usuarios y los grupos de Active Directory, recibida al sondear la red de Active Directory

c. Información sobre los dispositivos administrados y sus especificaciones técnicas, incluidas las especificaciones necesarias para identificar los dispositivos, las cuentas de los usuarios de los dispositivos y las sesiones de trabajo de estos usuarios

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

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

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

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

h. Ajustes de los componentes de Kaspersky Security Center y de las aplicaciones de Kaspersky administradas presentes en las directivas y en los perfiles de directivas

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

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

k. Categorías de aplicaciones creadas por el usuario

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

m. Detalles de los archivos almacenados en Copia de seguridad

n. Detalles de los archivos puestos en cuarentena

o. Detalles de los archivos solicitados por los especialistas de Kaspersky para realizar análisis detallados

p. Información sobre el estado y la activación de las reglas del Control de anomalías adaptativo

q. Detalles de los dispositivos (unidades de memoria, herramientas de transferencia de información, herramientas para copias de información impresas y buses de conexión) que se han instalado en el dispositivo administrado o que se han conectado a este y que fueron detectados por la función Control de dispositivos

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

s. Información sobre los errores encontrados al cifrarse los datos de dispositivos que utilizan la función de cifrado de datos de las aplicaciones de Kaspersky

t. Lista de los controladores de lógica programable (PLC) administrados

u. Detalles de los códigos de activación ingresados

v. Cuentas de usuario

w. Historial de revisiones de los objetos de administración

x. Registro de los objetos de administración eliminados

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

z. Configuración de usuario de Kaspersky Security Center Web Console

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

ab. Certificado para establecer una conexión segura entre los dispositivos administrados y los componentes de Kaspersky Security Center

28. Información cargada desde el dispositivo administrado cuando se utiliza la función de diagnóstico remoto: archivos de diagnóstico (archivos de volcado, archivos de registro, archivos de seguimiento, etc.) y los datos contenidos en estos archivos.

29. Datos que se requieren para integrar Kaspersky Security Center Cloud Console con un sistema SIEM y exportar a este los eventos:

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

  El usuario ingresa información 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 que se requieren para la interacción de Kaspersky Security Center Cloud Console con un entorno de nube:

a. Amazon Web Services (AWS):

- Id. de 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 la cuenta para el repositorio de Azure
- Clave de acceso de la cuenta para el repositorio de Azure

c. Google Cloud:

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

El usuario ingresa información 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 está disponible 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 del dispositivo al Servidor de administración a través del 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 del dispositivo al Servidor de administración a través del 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 ingresa 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 del 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 para dispositivos móviles
- 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"; a continuación, desplácese hacia abajo, hasta llegar a la sección sobre los datos de los dispositivos que se administran con la aplicación administrada pertinente. Para encontrar esta sección, también puede utilizar la función de búsqueda estándar de su navegador.

Datos del usuario procesados en forma local

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

Lista de datos del usuario que se procesan en forma local:

- Todos los datos que figuran en la sección de 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
- Datos de seguimiento 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 del Agente de red contienen datos aleatorios y pueden contener datos personales. Los archivos se almacenan en un formato no cifrado en el dispositivo en el que está instalado el Agente de red. Estos archivos no se transfieren a Kaspersky automáticamente. El usuario puede transferir estos datos a Kaspersky manualmente si el personal del servicio de soporte técnico los requiere para solucionar problemas con el funcionamiento 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 contrato de Kaspersky Security Center Cloud Console y el contrato de procesamiento de datos de Kaspersky Security Center Cloud Console al crear un espacio de trabajo para su 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 de las aplicaciones de Kaspersky

El Contrato de licencia de usuario final (en lo sucesivo denominado "Contrato de licencia" o "EULA") es un acuerdo vinculante, celebrado entre usted y AO Kaspersky Lab, en el que se estipulan los términos según los cuales puede utilizar las aplicaciones de Kaspersky.

Puede consultar los términos del Contrato de licencia de usuario final utilizando los siguientes métodos:

- en la ventana que se muestra al crear un paquete de instalación para una aplicación de Kaspersky;
- en el archivo license.txt que se encuentra en la carpeta de instalación de la aplicación de Kaspersky del dispositivo administrado.

Puede revocar su conformidad con el 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 esa aplicación.

Guía para reforzar la seguridad

Kaspersky Security Center Cloud Console es una aplicación alojada y mantenida por Kaspersky. No es necesario instalar Kaspersky Security Center Cloud Console en un equipo o servidor propios. A través de Kaspersky Security Center Cloud Console, el administrador puede instalar las aplicaciones de seguridad de Kaspersky en los dispositivos de una red corporativa, ejecutar tareas de análisis y actualización en forma remota y gestionar las directivas de seguridad de las aplicaciones administradas.

Kaspersky Security Center Cloud Console está diseñado para ejecutar tareas de administración y mantenimiento básicas en la red de una organización de forma centralizada. La aplicación proporciona al administrador acceso a información detallada sobre el nivel de seguridad de la red de la organización. Kaspersky Security Center 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 mayor protección para Kaspersky Security Center Cloud Console.

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

La Guía para reforzar la seguridad contiene la siguiente información:

- Configuración de cuentas para acceder a Kaspersky Security Center Cloud Console
- Administración de la protección de dispositivos cliente
- Configurar 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 pedirá que lea la versión breve de la Guía para reforzar la seguridad.

Tenga en cuenta que no puede usar Kaspersky Security Center Cloud Console hasta que confirme que ha leído la Guía para reforzar la seguridad.

Para leer la Guía para reforzar la seguridad:

1. Abra Kaspersky Security Center Cloud Console e inicie sesión. Kaspersky Security Center Cloud Console verifica si confirmó haber leído la versión actual de la Guía para reforzar la seguridad.

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

2. Realice una de las siguientes acciones:

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

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

Ahora puede trabajar con Kaspersky Security Center Cloud Console.

Cuando aparece una nueva versión de la Guía para reforzar la seguridad, Kaspersky Security Center Cloud Console 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 de conexión a Kaspersky Security Center Cloud Console
- Métodos de despliegue del Agente de red y el software de protección
- Uso de puntos de distribución
- Uso de Servidores de administración virtuales
- Uso de una jerarquía de Servidores de administración
- esquema de actualización de la base de datos antivirus.
- otros flujos de información.

Cuentas y autenticación

Uso de la verificación en dos pasos con Kaspersky Security Center Cloud Console

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

La verificación de dos pasos puede ayudarlo a aumentar la seguridad de su cuenta en Kaspersky Security Center Cloud Console. Si esta función está habilitada, deberá ingresar un código de seguridad único adicional cada vez que inicie sesión en Kaspersky Security Center Cloud Console, junto con su dirección de correo electrónico y contraseña. 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).

No recomendamos en absoluto instalar la app de autenticación en el mismo dispositivo desde el que se establece la conexión con Kaspersky Security Center Cloud Console. Puede instalar una app de autenticación en su dispositivo móvil.

Prohibición de guardar la contraseña de administrador

Si utiliza Kaspersky Security Center Cloud Console, **no recomendamos en absoluto** guardar la contraseña de administrador en el navegador instalado en el dispositivo del usuario.

Si el navegador está comprometido, un intruso puede obtener acceso a las contraseñas guardadas. Además, si se roba o se pierde un dispositivo de usuario con contraseñas guardadas, el intruso puede obtener acceso a los datos protegidos.

Restricción de la pertenencia a la función de Administrador principal

Recomendamos restringir la pertenencia al rol de Administrador principal.

De forma predeterminada, después de que un usuario crea un espacio de trabajo, la función de Administrador principal se asigna a este usuario. Es útil para la administración, pero es crítico desde el punto de vista de la seguridad, debido a que el rol de Administrador principal tiene una amplia gama de privilegios. La asignación de este rol a los usuarios debe estar estrictamente regulada.

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

Configurar los derechos de acceso a las funciones de la aplicación

Recomendamos usar 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 la creación de funciones de usuario estándar con un conjunto de derechos preestablecido y la asignación de esas funciones a los usuarios según su ámbito de responsabilidad.

Las principales ventajas del modelo de control de acceso basado en funciones:

- Facilidad de administración
- Jerarquía de funciones
- Enfoque de privilegios mínimos
- Segregación de deberes

Puede asignar funciones integradas a ciertos empleados en función de sus puestos o crear funciones completamente nuevas.

Al configurar 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:

- Administrar grupos de administración.
- Operaciones con el Servidor de administración.
- Instalación remota.
- Cambiar los parámetros para almacenar eventos y enviar notificaciones.

  Este privilegio le permite configurar notificaciones que ejecutan un script o un módulo ejecutable en el dispositivo del Servidor de administración cuando ocurra un evento.

Cuenta separada para la instalación remota de aplicaciones

Además de la diferenciación básica de derechos de acceso, recomendamos restringir la instalación remota de aplicaciones para todas las cuentas (excepto para el Administrador principal u otra cuenta especializada).

Recomendamos usar una cuenta aparte para la instalación remota de aplicaciones. Puede asignar un rol o permisos a la cuenta separada.

Administración 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 usa reglas automáticas para mover dispositivos, esto puede propagar directivas que otorguen más privilegios al dispositivo movido que los que tenía antes de la reubicación.

Además, mover un dispositivo cliente a otro grupo de administración puede provocar la propagación de la configuración de políticas. Estas configuraciones de políticas pueden ser indeseables para su distribución a dispositivos invitados y no confiables.

Esta recomendación no se aplica a la asignación inicial única de dispositivos a grupos de administración.

Requisitos de seguridad para puntos de distribución y puertas de enlace de conexión

Los dispositivos con Agente de red instalado pueden actuar como punto de distribución y realizar las siguientes funciones:

- Distribuir actualizaciones y paquetes de instalación recibidos del Servidor de administración a los dispositivos cliente dentro del grupo.
- Realizar la instalación remota de software de terceros y aplicaciones de Kaspersky en dispositivos cliente.
- Sondear la red para detectar nuevos dispositivos y actualizar la información disponible sobre los dispositivos de los que ya se tenía conocimiento.
- Actuar como un servidor proxy de KSN para dispositivos cliente.

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

Configurar 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. Es posible que estos parámetros no sean óptimos o incluso pueden estar prohibidos en su organización. Por lo tanto, recomendamos configurar las directivas y tareas creadas, y crear adicionales si es necesario para la red de su organización.

Especificar la contraseña para desactivar la protección y desinstalar la aplicación

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

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

Recomendamos encarecidamente habilitar la protección con contraseña para ejecutar la utilidad klmover y eliminar el Agente de red. Para habilitar 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 de Kaspersky Security Center Cloud Console, recomendamos habilitar el uso de Kaspersky Security Network (KSN) y aceptar la Declaración de KSN. Cuando mejora o actualiza 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 dar una respuesta oportuna a los problemas de seguridad, recomendamos configurar las funciones de supervisión y generación de informes.

Exportación de eventos a sistemas SIEM

Para obtener una detección rápida de problemas de seguridad antes de que se produzcan daños significativos, recomendamos usar la exportación de eventos en un sistema SIEM.

Notificaciones por correo electrónico de eventos de auditoría

Para obtener 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 publica.

Dado que estos eventos tienen lugar dentro del sistema, se puede esperar que no sean muchos, algo que resulta muy cómodos para enviarlos por correo.

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 el Agente de red, sugerimos que, de existir, aplique las prácticas de seguridad de la información recomendadas por el Center for Internet Security (CIS) para ajustar la configuración de estos sistemas de información.

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

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

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

Recomendaciones de seguridad para el sistema operativo Astra Linux

Si utiliza el sistema operativo Astra Linux, siga las recomendaciones de seguridad descritas en el "libro rojo" correspondiente a su versión de Astra Linux.

Recomendaciones para usar las aplicaciones de seguridad de Kaspersky

Usar la contraseña de KLAdmin en Kaspersky Endpoint Security para Windows

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

Una de las formas de restringir el acceso a Kaspersky Endpoint Security para Windows y sus parámetros es usar una cuenta KLAdmin. La cuenta KLAdmin es una cuenta de administrador con acceso sin restricciones a Kaspersky Endpoint Security para Windows. La cuenta KLAdmin tiene derecho a realizar cualquier acción protegida con contraseña en Kaspersky Endpoint Security para Windows. Los permisos para la cuenta KLAdmin no se pueden revocar. Puede configurar la contraseña de la cuenta KLAdmin en las propiedades de la directiva de Kaspersky Endpoint Security para Windows. El administrador de Kaspersky Endpoint Security para Windows es totalmente responsable del uso seguro de esta contraseña. Si su organización tiene una política de contraseñas propias, siga las directrices de esa política.

Estas son nuestras recomendaciones para proteger a una organización contra el robo de la contraseña de KLAdmin:

- **Requisitos generales**

  No utilice el nombre de la cuenta o parte del nombre como contraseña.

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

  Cree una contraseña de 10 caracteres o más.

- **Requisitos sobre el uso de varios tipos de caracteres**

  Establezca una contraseña compleja que contenga caracteres de diferentes categorías: letras minúsculas y mayúsculas, números y caracteres especiales.

- **Requisitos sobre la caducidad de la contraseña**

  Establezca la fecha mínima de caducidad de la contraseña en 90 días. Una nueva contraseña no debe coincidir con ninguna de las 24 contraseñas anteriores.

Interfaz de Kaspersky Security Center Cloud Console

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

La ventana de la aplicación contiene los siguientes elementos:

- Menú principal en la parte izquierda de la ventana
- un área de trabajo, en la parte derecha de la ventana

Menú principal

El menú principal contiene estas secciones:

- **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.
  - **Presentación y tutoriales**. Contiene videos sobre cómo configurar y usar Kaspersky Security Center Cloud Console y las aplicaciones de seguridad.

    En el navegador Mozilla Firefox, si se reproduce un video de la sección **Presentación y tutoriales** en una ventana emergente y luego ese video se abre en el modo de imagen en imagen, al cerrar el video en la ventana emergente, se cierra también el video abierto en el modo de imagen en imagen.
- **Servidor de administración**. Muestra el nombre del Servidor de administración al que se está conectado. Haga clic en el icono de configuración ( ) para abrir las propiedades del Servidor de administración.
- **Supervisión e informes**. Brinda una visión general de la infraestructura, los estados de protección y la información estadística.
- **Activos (dispositivos)**. Contiene herramientas para administrar dispositivos cliente, así como tareas y directivas de la aplicación de Kaspersky.
- **Usuarios y roles**. Le permite administrar usuarios y roles, configurar derechos de usuario mediante la asignación de roles a los usuarios y asociar perfiles de directivas con roles.
- **Operaciones**. Contiene una variedad de operaciones, incluidas la implementación de licencias de aplicaciones, la administración de parches y la administración de aplicaciones de terceros. Esto también le proporciona acceso a los repositorios de aplicaciones.
- **Descubrimiento 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 toda la gama de soluciones empresariales de Kaspersky y le permite seleccionar las que necesita y luego comprar esas soluciones en el sitio web de Kaspersky.
- **Configuración**. Contiene configuraciones 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 idioma o el tema de la interfaz.

- **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 usar 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, haga lo siguiente:

1. En el menú principal, vaya a **Configuración** → **Idioma**.
2. Seleccione uno de los idiomas de localización 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 agregado 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 agregar 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 agregar 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 agregar y eliminar elementos de los marcadores de la sección **Enlaces rápidos** situando el cursor del ratón sobre ellas y haciendo clic en el ícono 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

En esta sección se delinea el escenario de despliegue principal para Kaspersky Security Center Cloud Console. El proceso de despliegue comienza con la creación de un espacio de trabajo y culmina con la supervisión del estado de protección de la red.

Si necesita información para realizar un despliegue de Kaspersky Security Center en una infraestructura local, consulte la Ayuda en línea de Kaspersky Security Center.

Recomendamos reservar al menos un día de trabajo para completar este trabajo.

El escenario lo guía a través de lo siguiente:

- Comenzar a trabajar como administrador con un espacio de trabajo creado para su empresa
- Descubrir los dispositivos conectados a la red (de ser necesario, designará puntos de distribución e instalará paquetes de distribución manualmente en estos dispositivos)
- Desplegar las aplicaciones de Kaspersky administradas en los dispositivos cliente; configurar herramientas para proteger y supervisar la red y para actualizar periódicamente las aplicaciones, las bases de datos y los módulos de software de Kaspersky

Al concluir este escenario, su red estará protegida con las aplicaciones de Kaspersky. En ese punto, estará en condiciones de supervisar el estado de protección de la red.

Requisitos previos

Antes de comenzar:

- Familiarícese con la arquitectura de Kaspersky Security Center Cloud Console para comprender cómo interactúan los principales componentes de la 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 tiene pensado crear un espacio de trabajo comercial).

Etapas

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

1. **Configurar los puertos**

   Verifique que todos los puertos necesarios para la interacción entre su red y la infraestructura de Kaspersky se encuentren abiertos. Si planea utilizar la jerarquía de servidores de administración, asegúrese también de abrir todos los puertos necesarios para la interacción entre el Servidor de administración secundario (o los servidores de administración secundarios) y los dispositivos cliente.

2. **Crear el espacio de trabajo para la empresa**

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

3. **Ejecutar el asistente de inicio rápido**

Abra Kaspersky Security Center Cloud Console e inicie sesión. Cuando inicie sesión por primera vez, se le pedirá que ejecute el asistente de inicio rápido. El asistente de inicio rápido también se puede ejecutar manualmente en cualquier momento.

El asistente de inicio rápido le permitirá crear paquetes de instalación para el Agente de red y para las aplicaciones de seguridad. Necesitará estos paquetes de instalación para continuar con el despliegue de Kaspersky Security Center Cloud Console.

4. **Desplegar las aplicaciones de Kaspersky**

   Realice el despliegue inicial de las aplicaciones de Kaspersky. Como parte de este proceso, deberá realizar un sondeo de red. El sondeo permite determinar qué dispositivos cliente están presentes en la red. Para más información sobre el sondeo de red y sus opciones de configuración, consulte el escenario sobre el descubrimiento de dispositivos conectados a la red.

   Si planea desplegar Kaspersky Security for Windows Server, asegúrese de que las bases de datos de dicha aplicación estén actualizadas.

5. **Asignar las licencias necesarias a las aplicaciones de seguridad de Kaspersky**

   Una vez que las aplicaciones de seguridad de Kaspersky estén instaladas en los dispositivos administrados, deberá asegurarse de que cada una tenga la licencia necesaria. Para ello, tendrá que aplicar un código de activación a cada aplicación. Despliegue los códigos de activación a las aplicaciones de Kaspersky instaladas en los dispositivos administrados. Tiene varias opciones para agregar licencias a las aplicaciones de seguridad de Kaspersky.

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

   Configure la protección de la red a fin de ajustar las directivas y las tareas creadas con el asistente de inicio rápido.

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

   Para que la red nunca quede indefensa ante virus y otras amenazas, debe configurar un cronograma de actualización periódica para las bases de datos, las aplicaciones y los módulos de software de Kaspersky.

8. **Actualizar las aplicaciones de terceros y reparar sus vulnerabilidades de software (opcional)**

   Kaspersky Security Center Cloud Console puede utilizarse para administrar las actualizaciones de las aplicaciones de Microsoft instaladas en 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. **Configurar herramientas para supervisar el estado de protección de la red**

   Seleccione y configure widgets, informes y otras herramientas diseñadas para supervisar el estado de protección de la red.

Al concluir el proceso de despliegue y configuración de Kaspersky Security Center Cloud Console, podrá volcar su atención a supervisar el estado de protección de la red.

Administración de espacios de trabajo

En esta sección, se 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.

Primeros pasos con 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.

Creación de 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 usar Kaspersky Security Center Cloud Console.

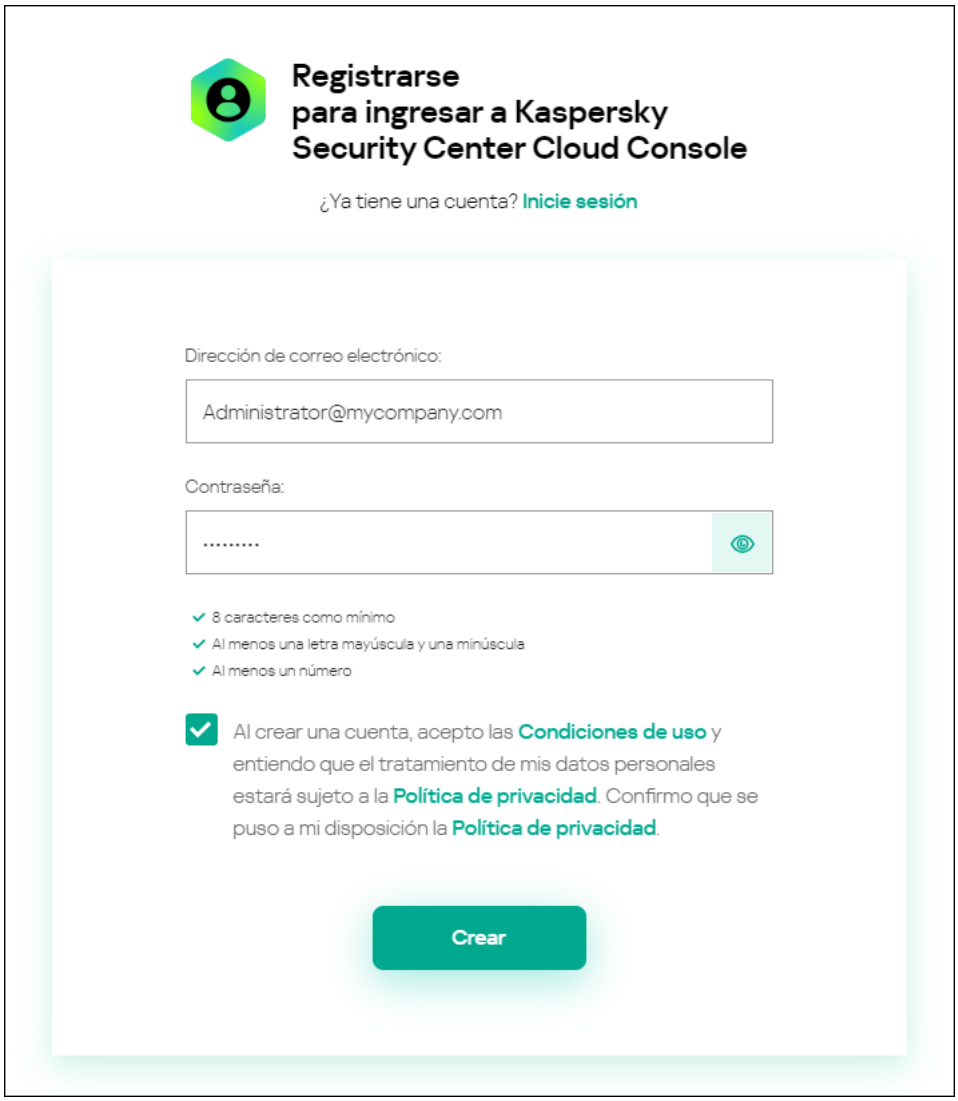
Para crear una cuenta en Kaspersky Security Center Cloud Console:

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

2. Haga clic en el **Crear 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 enlace **Política de privacidad** y lea con atención el texto de la Política 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. Se envía un mensaje desde Kaspersky 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 está 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 cambio, envíe una solicitud al servicio de soporte técnico de Kaspersky. En la solicitud, brinde información sobre la empresa que desee registrar y el espacio de trabajo que desee crear.

Antes de iniciar, asegúrese de saber lo siguiente:

- El nombre de la empresa en la cual tiene la intención de usar la solución de software.
- El país en el que 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 su 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 **Siguiente**.
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 leyó 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.

   Complete 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 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 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 ingresar 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, ingrese 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 están completos.

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 cambio, envíe una solicitud al servicio de soporte técnico de Kaspersky. Cada espacio de trabajo admite un máximo de 25 000 dispositivos.

En la solicitud, incluya los siguientes datos:

- **Correo electrónico del usuario**: la dirección de correo electrónico del usuario que se registró en Kaspersky Security Center Cloud Console. Este usuario tendrá 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. En la solicitud, incluya información sobre la empresa y sobre el espacio de trabajo.

- **Nombre de la 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**: la cantidad total de dispositivos cliente que buscará proteger en el nuevo espacio de trabajo (incluya en este recuento el número de dispositivos móviles).

- **País del espacio de trabajo**: el país en el que desea que esté ubicado el nuevo espacio de trabajo. De este parámetro depende el centro de datos elegido para almacenar el espacio de trabajo.

  El **país de la empresa** y el **país del espacio de trabajo** pueden ser los mismos.

- **Código de activación**: el código de activación que recibió al comprar Kaspersky Security Center Cloud Console. Asegúrese de que su licencia alcance para cubrir todos los dispositivos clientes que desee proteger.

Una vez que envíe su solicitud, los especialistas de Kaspersky se ocuparán de registrar la empresa y crearán un espacio de trabajo para ella. Recibirá un aviso por correo electrónico cuando el espacio de trabajo esté listo. 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 su espacio de trabajo de Kaspersky Security Center Cloud Console, haga lo siguiente:

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, ingrese 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 para la que es administrador y la lista de sus espacios de trabajo.

4. Haga clic en el nombre del espacio de trabajo requerido o en el vínculo **Ir al espacio de trabajo** para ingresar a este.

   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 sufriera cambios desde el momento en el que aceptó los términos y condiciones, la página del portal mostrará los documentos con los cambios.

   Haga lo siguiente:

   a. Lea con atención los documentos en pantalla.

   b. Si está de acuerdo con los términos y condiciones de estos documentos, marque las casillas que se encuentran al lado de la lista de documentos y haga clic en el botón **Acepto los términos**.

      > 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.

Volver 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,

en el menú principal, vaya a la configuración de su cuenta y seleccione **Administrar espacios de trabajo**.

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

Cerrar sesión en Kaspersky Security Center Cloud Console

Cada vez que termine de utilizar Kaspersky Security Center Cloud Console, debe cerrar su sesión en forma segura.

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 aparece la página de inicio de sesión. Puede cerrar esta página del navegador, si es necesario. 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 empresa y la lista de espacios de trabajo registrados bajo su cuenta en Kaspersky Security Center Cloud Console, cambiar la información sobre la empresa y los espacios de trabajo, y eliminar un espacio de trabajo y una compañía.

En la actualidad, solo puede registrar una empresa y crear un espacio de trabajo. En versiones futuras 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 independiente 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 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, ingrese 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 mostrará 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 esa empresa decidió de 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 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, ingrese 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 ícono **Eliminar** (🗑).

   Se abre 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 pudo marcar un espacio de trabajo para eliminarlo, comuníquese con el Servicio de soporte técnico de Kaspersky. Después de que 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 que se marcan para la eliminación pueden permanecer en ese estado durante un período de siete días luego de haber sido marcados. Después de siete días, son automáticamente eliminados.

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 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, ingrese 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 abre la ventana **Eliminar espacio de trabajo**.
5. En la ventana **Eliminar espacio de trabajo**, ingrese el ID del espacio de trabajo que desea eliminar.

   Se le solicita el ID del espacio de trabajo para asegurarse de que no eliminará equivocadamente el espacio de trabajo. Después de eliminar un espacio de trabajo, no se puede restaurar.

   El ID del 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

Los espacios de trabajo de Kaspersky Security Center Cloud Console se eliminan automáticamente en estos momentos:

- treinta días después de que caduca una licencia de prueba;
- noventa días después de que caducan todas las licencias comerciales o de suscripción disponibles en el repositorio del Servidor de administración;
- noventa días después de que se elimina la última clave de licencia (activa, de reserva o no utilizada) agregada al repositorio manualmente.

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 haya marcado para su eliminación.

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

Para cancelar la eliminación de un espacio 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, ingrese 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 seguir 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.

Otorgar 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, ingrese 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 agregado. 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, ingrese 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 ícono **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.

Restablecer 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 **¿Olvidó su contraseña?**.
4. Ingrese la dirección de correo electrónico que especificó al momento de crear la cuenta.
5. Haga clic en **Siguiente**.
6. Se envía un mensaje desde Kaspersky 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 configuró una pregunta secreta, respóndala.

   Si configuró la verificación en dos pasos, ingrese 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).
9. En la ventana que se abre, escriba una nueva contraseña.
10. Haga clic en **Guardar**.

    La nueva contraseña para iniciar sesión en Kaspersky Security Center Cloud Console está guardada.

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. Comuníquese con el Servicio de 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 enlace 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**, escriba su correo electrónico nuevo.

   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. Se envía un mensaje desde Kaspersky 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 enlace 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. No podrá guardar la contraseña nueva hasta que cumpla con los requisitos.

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. Marque o desmarque la casilla **Solicitar automáticamente el cambio de contraseña cada 180 días**.

   Esta casilla está marcada de forma predeterminada.

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.

Usar la verificación en dos pasos

En esta sección se describe la verificación en dos pasos, que puede ayudarle a mejorar la seguridad de su cuenta en Kaspersky Security Center Cloud Console.

Acerca de la verificación en dos pasos

La verificación de dos pasos puede ayudarlo a aumentar la seguridad de su cuenta en Kaspersky Security Center Cloud Console. Si esta función está habilitada, deberá ingresar un código de seguridad único adicional cada vez que inicie sesión en Kaspersky Security Center Cloud Console, junto con su dirección de correo electrónico y contraseña. Con la verificación en 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. A su vez, cuando la verificación en dos pasos está habilitada, debe ingresar un código de seguridad único adicional si olvida la 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 app de autenticación que se instala en su teléfono móvil.

  Le recomendamos que configure la verificación en dos pasos con una app 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. Verifique el cumplimiento del GDPR y las políticas de privacidad de las aplicaciones antes de usarlas. Kaspersky no está, de ninguna manera, patrocinado por ninguno de los propietarios de estas aplicaciones, ni está respaldado por ellos ni afiliado a ellos.

  > Microsoft Authenticator solo se puede instalar en dispositivos móviles.

  Le recomendamos que además instale una aplicación de autenticación en un dispositivo que no sea un 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 app 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: configurar la verificación en dos pasos

La verificación en 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 en dos pasos de su cuenta.

El escenario se divide en etapas:

1. **Agregar su número de teléfono**

   En esta etapa, debe configurar la verificación en dos pasos por SMS.

2. **Instalar y configurar una app de autenticación**

   Instale y configure una aplicación de autenticación.

   Le recomendamos encarecidamente 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.

   Le recomendamos que además instale una aplicación de autenticación en un dispositivo que no sea un teléfono móvil. Esto le permitirá iniciar sesión en su cuenta incluso si le robaran su teléfono móvil o lo perdiera.

3. **Cambiar su número de teléfono**

   Si es necesario, puede cambiar el número de teléfono para la verificación en dos pasos.

Configuración de la verificación en dos pasos mediante SMS

Para configurar la verificación en dos pasos por SMS:

1. En Kaspersky Security Center Cloud Console, haga clic en el enlace 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 utilizar 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**.

Se configuró la verificación en dos pasos. Ahora, cada vez que inicie sesión con su dirección de correo electrónico y contraseña, o si olvida la contraseña, deberá ingresar un código de seguridad único que obtendrá mediante SMS al número de teléfono especificado.

Ya puede instalar la aplicación de autenticación y configurarla, cambiar el número de teléfono o deshabilitar la verificación en dos pasos.

Configuración de la verificación en dos pasos mediante una aplicación de autenticación

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 deshabilita la verificación en dos pasos a través de su número de teléfono móvil, se deshabilitará de forma automática la verificación mediante la aplicación de autenticación. Luego de que configure la verificación mediante SMS y a través de una aplicación, podrá seleccionar un método de verificación en la página de inicio de sesión o si olvida su contraseña.

Para configurar la verificación en dos pasos a través de una app de autenticación:

1. Configure la verificación en dos pasos mediante SMS.

2. Descargue, instale y ejecute la app de autenticación que desea usar.

   Solo probamos la compatibilidad de Google Authenticator y Microsoft Authenticator con Kaspersky Security Center Cloud Console, y estas aplicaciones no tenían costo de uso en ese momento. Las interfaces de estas aplicaciones pueden no estar disponibles en su idioma. Verifique el cumplimiento del GDPR y las políticas de privacidad de las aplicaciones antes de usarlas. Kaspersky no está, de ninguna manera, patrocinado por ninguno de los propietarios de estas aplicaciones, ni está respaldado por ellos ni afiliado a ellos.

   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 app 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 enlace 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 generará 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**.

Se configura la verificación de dos pasos a través de la aplicación autenticadora. Ahora, cada vez que inicie sesión con su dirección de correo electrónico y contraseña, o si olvida la contraseña, deberá ingresar un código de seguridad único que se genera en la aplicación de autenticación.

Ya puede deshabilitar el uso de una aplicación de autenticación o deshabilitar por completo la verificación en dos pasos.

Cambiar 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 enlace 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 vínculo **Cambiar 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.

Deshabilitación de la verificación en 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 configuró la verificación en dos pasos mediante SMS, puede deshabilitar la verificación en dos pasos. Si configuró la verificación en dos pasos mediante una aplicación de autenticación, puede deshabilitar el uso de la aplicación o puede deshabilitar por completo la verificación en dos pasos.

Para deshabilitar el uso de la app de autenticación, haga lo siguiente:

1. En Kaspersky Security Center Cloud Console, haga clic en el enlace 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 deshabilitará el uso de la aplicación de autenticación. Se eliminará la configuración de la verificación en dos pasos a través de una app de autenticación. Ahora puede eliminar cuentas en las aplicaciones autenticadoras.

Luego, podrá volver a configurar la verificación en dos pasos a través de una aplicación de autenticación.

Para desactivar por completo la verificación en dos pasos:

1. En Kaspersky Security Center Cloud Console, haga clic en el enlace 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 deshabilitará la verificación en dos pasos. Si ha utilizado la verificación en dos pasos a través de una app de autenticación, se eliminará la configuración de la verificación en dos pasos. Ahora, puede eliminar las cuentas de la app de autenticación.

Luego, podrá volver a configurar la verificación en dos pasos.

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 fue 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 enlace 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 la 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

País en el que 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 (Isla del Príncipe Eduardo)	México o Brasil
Canadá (Quebec)	México o Brasil
Albania	Irlanda
Bosnia y 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
Rumania	Irlanda
Serbia	Irlanda
Federación Rusa	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 (Yukon)	México o Brasil
Canadá (Saskatchewan)	México o Brasil
México	México o Brasil
Otros países	Irlanda

Acceso a los servidores DNS públicos

Si no es posible acceder a los servidores de Kaspersky mediante los servidores DNS del sistema, Kaspersky Security Center Cloud Console puede utilizar los siguientes servidores DNS públicos en el siguiente orden:

1. Servidores DNS públicos de Google (8.8.8.8)
2. Servidores DNS de Cloudflare (1.1.1.1)
3. Servidores DNS de Alibaba Cloud (223.6.6.6)
4. Servidores DNS de Quad9 (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

Las solicitudes realizadas a estos servidores DNS pueden contener direcciones de dominio y la dirección IP pública de dispositivos cliente, ya que el Agente de red establece una conexión TCP/UDP con los servidores DNS. Cuando 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: Crear una jerarquía de servidores de administración que se administren con Kaspersky Security Center Cloud Console

Las acciones que se describen en este escenario le permitirán crear una jerarquía de servidores de administración que se administren con Kaspersky Security Center Cloud Console. En la jerarquía resultante, Kaspersky Security Center Cloud Console tendrá el rol de Servidor de administración principal. Una vez que cree la jerarquía, podrá usarla para migrar dispositivos administrados y otros objetos de Kaspersky Security Center a Kaspersky Security Center Cloud Console o para administrar dispositivos y servidores de administración secundarios a través de Kaspersky Security Center Cloud Console.

Kaspersky Security Center Cloud Console solo puede actuar como Servidor de administración principal. Los servidores de administración locales, por su parte, solo pueden actuar como servidores de administración secundarios. Este es el único esquema jerárquico que puede utilizar.

Requisitos previos

Antes de comenzar, asegúrese de que se cumplan los siguientes requisitos previos:

- El Servidor de administración local se ha actualizado a la versión 12 o una posterior.
- Kaspersky Security Center Web Console se encuentra instalado en el Servidor de administración local.
- Se encuentran instalados los complementos web para las aplicaciones que planea administrar con Kaspersky Security Center Cloud Console.
- Actualizar las aplicaciones administradas a versiones compatibles con Kaspersky Security Center Cloud Console.
- El Servidor de administración principal no está designado como origen de actualizaciones en la tarea "Descargar actualizaciones en el repositorio del Servidor de administración" del Servidor de administración local. De no cumplirse este requisito, haga los cambios necesarios en la configuración de la tarea.

Una vez que cree la jerarquía, las directivas y las tareas que estén vigentes en Kaspersky Security Center Cloud Console se aplicarán en el Servidor de administración secundario y reemplazarán sus directivas y tareas existentes. Si no quiere que suceda esto, antes de crear la jerarquía, elimine todas las directivas y tareas de Kaspersky Security Center Cloud Console. Como alternativa, cambie el estado de cada directiva de Kaspersky Security Center Cloud Console a **Inactiva** y deshabilite la opción **Distribuir a Servidores de administración secundarios y virtuales** en la configuración de cada tarea de Kaspersky Security Center Cloud Console.

Podrá eliminar la jerarquía de servidores de administración en cualquier momento.

Etapas en la creación de la jerarquía

El escenario básico está pensado para un Servidor de administración secundario al que no se puede acceder a través de Internet. De no ser este el caso, tenga presente que las acciones descritas en algunos de los pasos podrían requerir cambios. También deberá omitir algunos pasos.

El proceso para crear una jerarquía de servidores de administración comprende las siguientes etapas:

1. **Obtener el certificado del Servidor de administración secundario**

   Omita este paso si se puede acceder al Servidor de administración secundario a través de Internet.

   En la instancia local de Kaspersky Security Center Web Console, abra las propiedades del Servidor de administración. Luego, en la pestaña **General**, abra la sección **General**. Haga click en el enlace **Ver el certificado del Servidor de administración**. El archivo del certificado, en formato CER, se guardará automáticamente en la carpeta definida en los ajustes del navegador.

2. **Obtener los ajustes de conexión y los certificados de Kaspersky Security Center Cloud Console**

   Omita este paso si se puede acceder al Servidor de administración secundario a través de Internet.

   En Kaspersky Security Center Cloud Console, abra las propiedades del Servidor de administración. Luego, en la pestaña **General**, abra la sección **Jerarquía de Servidores de administración**. Se muestran los siguientes ajustes de conexión:

   - Dirección de HDS

     Dirección web utilizada para conectarse a Hosted Discovery Service (HDS).

   - Puerto de HDS

     Número del puerto utilizado para conectarse a HDS.

   En esta sección, encontrará también dos vínculos:

   - Ver el certificado del Servidor de administración

     Si hace clic en este vínculo, se iniciará la descarga de la clave pública correspondiente al certificado de la instancia de Kaspersky Security Center Cloud Console.

   - Certificado de CA raíz de HDS

     Si hace clic en este vínculo, se iniciará la descarga de un archivo en formato .pem. El archivo contiene una lista con los certificados raíz de confianza que han emitido las entidades de certificación (CA, por sus siglas en inglés). El Servidor de administración secundario necesita y utiliza este archivo para verificar el certificado de HDS.

   Copie los ajustes de conexión manualmente (use el portapapeles o el método que prefiera) y guárdelos en un archivo de cualquier formato apropiado. Haga clic en el vínculo **Ver el certificado del Servidor de administración** y espere a que se descargue el archivo del certificado. Haga clic en el vínculo **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 entidades de certificación. Los archivos se guardarán en la carpeta especificada en la configuración del navegador.

3. **Seleccionar el Servidor de administración secundario que se conectará**

En las propiedades del Servidor de administración, vaya a la pestaña **Servidores de administración**. En la jerarquía de grupos de administración, active la casilla de verificación ubicada junto al grupo de administración en el que desee incluir el Servidor de administración secundario y sus dispositivos administrados. Haga click en el botón **Conectar Servidor de administración secundario**.

En la página que se abre, en el campo **Nombre para mostrar del Servidor de administración secundario**, escriba el nombre que identificará al Servidor de administración secundario en la jerarquía. Este nombre es solo para su comodidad; no es necesario que coincida con el nombre real del Servidor de administración secundario. Haga clic en **Siguiente**.

Si se puede acceder al Servidor de administración secundario a través de Internet, especifique también 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 elija el archivo .pem que obtuvo del Servidor de administración secundario. Haga clic en **Siguiente**.

4. **Habilitar y configurar un servidor proxy**

Las acciones que se describen en este paso son opcionales. Realícelas solo si su conexión requiere el uso de un servidor proxy.

Haga clic en **Siguiente**. Si necesita hacerlo, en la página **Configuración de conexiones y autenticación**, puede habilitar y configurar el uso de un servidor proxy. Active la casilla de verificación **Usar servidor proxy** e introduzca los siguientes valores del servidor proxy:

- Dirección del servidor proxy

  La dirección del servidor proxy.

- Nombre de usuario

  El nombre de usuario que permite iniciar sesión en el servidor proxy.

- Contraseña

  La contraseña que permite iniciar sesión en el servidor proxy.

5. **Configurar los ajustes de autenticación y agregar el 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 que permite iniciar sesión en el Servidor de administración secundario.

- Contraseña

  La contraseña que permite iniciar sesión en el Servidor de administración secundario.

Haga clic en **Siguiente** y espere a que el Servidor de administración secundario aparezca en la jerarquía.

Si se puede acceder al Servidor de administración secundario a través de Internet, el mismo se conectará 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 los demás pasos.

Si no se puede acceder al Servidor de administración secundario a través de Internet, el mismo se volverá visible, pero deberá realizar acciones adicionales en el Servidor de administración secundario para poder controlarlo.

6. **Configurar la conexión en la instancia local de Kaspersky Security Center Web Console**

En la instancia local de Kaspersky Security Center Web Console, abra las propiedades del Servidor de administración. Luego, en la pestaña **General**, abra la sección **Jerarquía de Servidores de administración**. Marque la casilla **Este Servidor de administración es un servidor secundario en la jerarquía**. En la lista **Tipo de Servidor de administración principal**, seleccione la opción **Kaspersky Security Center Cloud Console**.

Kaspersky Security Center Web Console verificará si el Servidor de administración principal es el origen de actualizaciones configurado en la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Si el Servidor de administración principal es el origen de actualizaciones, verá una advertencia al respecto y un vínculo para acceder a la configuración de la tarea. Puede modificar la configuración y continuar creando la jerarquía, o puede omitir esta acción y continuar creando la jerarquía.

En el grupo **Configuración para establecer conexión entre los Servidores de administración principal y secundario**, defina los valores de los siguientes ajustes:

- Dirección del servidor HDS (tomada del Servidor de administración principal en Cloud Console)

  Ingrese la dirección del servidor HDS en formato de nombre de dominio completo (FQDN). Copió y guardó esta información al revisar las propiedades del Servidor de administración en Kaspersky Security Center Cloud Console.

- Puertos del servidor HDS

  Ingrese el número del puerto (o los números de los puertos) del servidor HDS. Copió y guardó esta información al revisar las propiedades del Servidor de administración en Kaspersky Security Center Cloud Console.

7. **Agregar los certificados en el Servidor de administración secundario**

Haga clic en el botón **Especificar el certificado del Servidor de administración principal** y elija el archivo de certificado que obtuvo al consultar las propiedades del Servidor de administración en Kaspersky Security Center Cloud Console.

Haga clic en el botón **Especificar los certificados de Hosted Discovery Service** y elija el archivo .pem que obtuvo al consultar las propiedades del Servidor de administración en Kaspersky Security Center Cloud Console.

Si habilitó el uso de un servidor proxy al conectar el Servidor de administración secundario en Kaspersky Security Center Cloud Console, active la casilla de verificación **Usar servidor proxy** y copie los ajustes que especificó para el servidor proxy en Kaspersky Security Center Cloud Console.

También puede activar la casilla **Conectar el Servidor de administración principal a un Servidor de administración secundario en DMZ** si el Servidor de administración secundario está en una zona desmilitarizada (DMZ).

El Servidor de administración secundario se conectará al Servidor de administración principal.

Resultados

Cuando termine de realizar estos pasos, puede asegurarse de que la jerarquía se haya creado correctamente. Para ello, verifique lo siguiente:

- Las directivas activas del Servidor de administración principal están vigentes en el Servidor de administración secundario. Las tareas del Servidor de administración principal se distribuyeron al Servidor de administración secundario. Las tareas de grupo que tienen habilitada la opción **Distribuir a Servidores de administración secundarios y virtuales** (de existir tales tareas) también se distribuyeron al Servidor de administración secundario.

- Los ajustes que no se permite modificar en las directivas del Servidor de administración principal tampoco se pueden modificar en las directivas del Servidor de administración secundario.

- Las directivas aplicadas por el Servidor de administración principal aparecen 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 aparecen en la lista de tareas del Servidor de administración secundario (**Activos (dispositivos)** → **Tareas**).

- Las directivas y las 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 grupos de administración, el Servidor de administración secundario aparece dentro del grupo que seleccionó al agregarlo.

Migración a Kaspersky Security Center Cloud Console

En esta sección se describe el proceso de migración a Kaspersky Security Center Cloud Console desde:

- Kaspersky Security Center Web Console versión 12 (o posterior), instancia 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

En esta sección, se describe el proceso para migrar a Kaspersky Security Center Cloud Console desde una instancia local de Kaspersky Security Center Web Console versión 12 (o posterior).

Métodos para migrar a Kaspersky Security Center Cloud Console

La característica de migración permite transferir dispositivos administrados con Kaspersky Security Center y ceder el control de los mismos a Kaspersky Security Center Cloud Console. Los dispositivos administrados migrarán sin que se pierdan sus ajustes más importantes (como la pertenencia a grupos de administración); tampoco se perderá ningún objeto esencial, como las directivas y las tareas relacionadas 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 afines a Kaspersky Security Center Cloud Console incluso si el Servidor de administración local no es un Servidor de administración secundario de Kaspersky Security Center Cloud Console.
  - Si Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console están abiertos en diferentes dispositivos físicos, puede que necesite transferir archivos utilizando una unidad extraíble, por correo electrónico, por medio de carpetas compartidas o de cualquier otra manera que resulte conveniente.

  > También puede realizar migración con Servidores de administración virtuales si su red los incluye.

- Migración con una jerarquía de servidores de administración:
  - Permite transferir dispositivos administrados y objetos afines a Kaspersky Security Center Cloud Console utilizando solamente la interfaz de Kaspersky Security Center Cloud Console. No es necesario transferir ningún archivo por medios físicos.
  - Requiere que el Servidor de administración local actúe como Servidor de administración secundario de Kaspersky Security Center Cloud Console. La jerarquía necesaria se puede crear antes de comenzar con la migración.

En lo que respecta al cifrado de disco completo, Kaspersky Security Center Cloud Console solo es compatible con BitLocker.

Escenario: Migración sin una jerarquía de servidores de administración

En esta sección, se describe el proceso para migrar los dispositivos administrados y los objetos relacionados con estos (como las directivas, las tareas y los informes) de una instancia local de Kaspersky Security Center Web Console a Kaspersky Security Center Cloud Console. Puede incluir un solo grupo de administración en el alcance de la migración para restaurar ese mismo grupo de administración en Kaspersky Security Center Cloud Console.

El grupo migrado debe contener los dispositivos administrados que utilicen un mismo sistema operativo. Si tiene dispositivos con diferentes sistemas operativos o con diferentes distribuciones de Linux en su red, asígnelos a grupos de administración independientes y migre cada grupo por separado.

Una vez que finalice la migración, las instancias del Agente de red que estén dentro del alcance de la migración se actualizarán y quedarán bajo el mando de Kaspersky Security Center Cloud Console.

En el proceso de migración que se aborda en los siguientes pasos, se asume que no existe una jerarquía de servidores de administración, es decir, que no se ha establecido 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 la versión 12.1 (o una posterior) de Kaspersky Security Center Web Console.
- Actualice el Agente de red en los dispositivos administrados a la versión 12 o una posterior.
- En los dispositivos con Windows, use el Agente de red sin contraseña de desinstalación.

  Si ya había definido esta contraseña, realice una de las siguientes acciones en Kaspersky Security Center Web Console:

  - Deshabilite la opción **Utilizar contraseña de desinstalación** en los ajustes de la directiva del Agente de red.
  - Desinstale el Agente de red en forma remota con la tarea *Desinstalar aplicación de forma remota*. En el campo **Aplicación para desinstalar** de la tarea, seleccione **Agente de red de Kaspersky Security Center**. No olvide ingresar la contraseña de desinstalación.
- Actualice las aplicaciones administradas a versiones que sean 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 de las aplicaciones que planee 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 toda la información que Kaspersky Endpoint Security para Windows haya cifrado (a nivel de disco o de archivo) en los dispositivos con Windows administrados. Luego, deshabilite la función de cifrado en esos dispositivos (puede hacer esto en forma local o a través de la directiva de la aplicación). Para obtener más información, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

  Si durante el proceso de migración se detecta que un dispositivo con Windows aún tiene archivos o carpetas cifrados mediante Kaspersky Endpoint Security para Windows, se cancelará la actualización del Agente de red. A través de una notificación, se le pedirá que descifre todos los datos del dispositivo y que desactive la función de cifrado.

Kaspersky Security Center Cloud Console admite un máximo de 25 000 dispositivos administrados por Servidor de administración.

Etapas de la migración

La migración a Kaspersky Security Center Cloud Console se divide en las siguientes etapas:

1. **Planificar el alcance de la migración y verificar que se satisfagan los requisitos previos**

   Estime el alcance del proceso de migración, es decir, revise el grupo de administración que desee exportar y evalúe la cantidad de dispositivos administrados que contiene. Asegúrese de haber completado correctamente todas las actividades definidas como requisitos previos para la migración.

2. **Exportar los dispositivos administrados, los objetos y los ajustes de Kaspersky Security Center Web Console**

   Use el Asistente de migración de la instancia local de Kaspersky Security Center Web Console para exportar los dispositivos administrados y sus objetos.

   El tamaño máximo del archivo de exportación es de 4 GB.

3. **Importar el archivo de exportación en Kaspersky Security Center Cloud Console**

   Transfiera la información de los dispositivos administrados y los objetos a Kaspersky Security Center Cloud Console. Utilice para ello el Asistente de migración de Kaspersky Security Center Cloud Console. Esta herramienta le permitirá importar el archivo de exportación y crear un paquete de instalación independiente para el Agente de red.

4. **Reinstalar el Agente de red en los dispositivos administrados**

   Regrese al Asistente de migración en la instancia local de Kaspersky Security Center Web Console para crear una tarea de instalación remota. Podrá utilizar esta tarea (a la primera oportunidad posible o cuando resulte conveniente) para reinstalar el Agente de red en los dispositivos administrados y completar el proceso de migración.

Resultados

Al finalizar la migración, puede asegurarse de que el proceso se haya realizado correctamente. Para ello, verifique lo siguiente:

- 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 conservaron todos los ajustes que estaban en vigencia antes de la migración.

Asistente de migración

En esta sección, encontrará información sobre el Asistente de migración de Kaspersky Security Center Cloud Console y de Kaspersky Security Center Web Console versión 12 (o posterior).

Paso 1. Exportar los dispositivos administrados, los objetos y los ajustes de Kaspersky Security Center Web Console

Para migrar dispositivos administrados de Kaspersky Security Center Web Console a Kaspersky Security Center Cloud Console, lo primero que debe hacer es crear un archivo de exportación con información sobre la jerarquía de grupos de administración creados en el actual Servidor de administración local. El archivo de exportación también debe contener información sobre los objetos y la configuración de esos objetos. Más adelante, importará este archivo en Kaspersky Security Center Cloud Console.

El tamaño máximo del archivo de exportación es de 4 GB.

Para exportar objetos y la configuración de esos objetos desde Kaspersky Security Center Web Console:

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**. La página 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 ícono del corchete angular (>) ubicado junto al nombre del grupo **Dispositivos administrados** para expandir la jerarquía de grupos de administración. Seleccione el grupo de administración que desee exportar.

   Tras completar una migración de dos grupos de administración de una instancia local de Kaspersky Security Center a Kaspersky Security Center Cloud Console, las tareas de instalación remota de esos grupos se mostrarán con el mismo nombre.

4. Seleccione las aplicaciones administradas cuyas directivas y tareas quiera transferir a Kaspersky Security Center Cloud Console junto con los objetos del grupo. Para seleccionar las aplicaciones administradas a las que correspondan los objetos que quiera exportar, active las casillas de verificación adyacentes a los nombres de esas aplicaciones en la lista.

   Aunque el Servidor de administración de Kaspersky Security Center estará incluido en la lista, sus directivas no se exportarán si activa la casilla de verificación correspondiente.

Para verificar si sus aplicaciones administradas son compatibles con Kaspersky Security Center Cloud Console, haga clic en el vínculo correspondiente. Al hacerlo, se abrirá un tema de la Ayuda en línea en el que se enumeran las aplicaciones administradas por Kaspersky Security Center Cloud Console.

Si selecciona aplicaciones incompatibles con Kaspersky Security Center Cloud Console, sus directivas y tareas se exportarán e importarán de todos modos, pero no podrá administrarlas en Kaspersky Security Center Cloud Console porque no tendrá los complementos dedicados que se requieren.

5. Revise la lista de objetos del grupo que se exportarán por defecto. De ser necesario, especifique objetos que no estén vinculados al grupo, pero que quiera exportar con el grupo de administración seleccionado. Para configurar el alcance 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. La 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 elige una tarea global asociada a una selección de objetos específica, también se exportará la selección.

     Aunque aparezcan en la lista, las tareas globales del Servidor de administración no se pueden exportar. Si selecciona estas tareas, el alcance de la exportación no cambiará. Las tareas de instalación remota también quedan excluidas 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**

     Una lista editable con las instancias de los informes que se exportarán.

     Si elige un informe asociado a una selección de objetos específica, también se exportará la selección.

     Kaspersky Security Center Cloud Console contiene el mismo conjunto de plantillas de informes que Kaspersky Security Center Web Console. Por ello, al momento de elegir los informes para exportar, solamente podrá seleccionar aquellos que haya creado o reconfigurado manualmente.

   - **Objetos de grupo**

La lista de objetos del grupo que se exportarán por defecto. De manera predeterminada, se exportarán en su totalidad los siguientes objetos relacionados con el grupo de administración seleccionado:

- 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 creó una etiqueta en Kaspersky Security Center Web Console, pero nunca la asignó a un dispositivo, no se la exportará. Las reglas de 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 exportarán.

- 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 exportarán.

También puede evitar que se exporten ciertos tipos de objetos no vinculados al grupo:

- Si no desea que se exporten los roles personalizados (es decir, aquellos creados por el usuario únicamente), active la casilla de verificación **Excluir roles personalizados de la exportación**.
- Si no desea que se exporten los usuarios internos ni los grupos de seguridad, active la casilla de verificación **Excluir usuarios internos y grupos de seguridad de la exportación**.
- Si no desea que se exporten las categorías de aplicaciones personalizadas con contenido agregado manualmente, active la casilla de verificación **Excluir categorías de aplicaciones personalizadas de la exportación**.

Si transfiere dispositivos con diferentes sistemas operativos a Kaspersky Security Center Cloud Console, solo tendrá que migrar los objetos que no estén vinculados a un grupo una vez.

El Asistente de migración contará la cantidad de dispositivos administrados incluidos en el grupo de administración seleccionado. Si el número es superior a 10 000, verá un mensaje de error. No podrá hacer clic en el botón **Siguiente**, que estará atenuado, hasta que reduzca al máximo permitido (o menos) la cantidad de dispositivos administrados del grupo de administración seleccionado.

6. Después de definir el alcance de la migración, haga clic en **Siguiente** para comenzar el proceso de exportación. Se abre la página **Creación del archivo de exportación**, en la que puede ver el progreso de exportación de cada tipo de objeto incluido en el alcance de la migración. Espere a que los íconos de actualización (↻) ubicados junto a los elementos de la lista de objetos cambien por marcas de verificación verdes (✓). Cuando finalice la exportación, el archivo de exportación se guardará automáticamente en la carpeta de descargas predeterminada de su navegador. Encontrará el nombre del archivo en la parte inferior de la ventana del navegador.

7. Cuando aparezca la página **La exportación se completó correctamente**, pase a la siguiente etapa, que se desarrolla en Kaspersky Security Center Cloud Console.

Si utiliza Kaspersky Security Center Web Console y Kaspersky Security Center Cloud Console en dispositivos diferentes, tendrá que copiar el archivo de exportación a una unidad extraíble o elegir otra forma de transferirlo.

Paso 2. Importar el archivo de exportación en Kaspersky Security Center Cloud Console

Para que se transfiera la información de los dispositivos administrados, los objetos y la configuración de los objetos que exportó de Kaspersky Security Center Web Console, debe importarla en la instancia de Kaspersky Security Center Cloud Console desplegada en su espacio de trabajo. Una vez que lo haga, podrá crear y utilizar un paquete de instalación independiente para reinstalar el Agente de red en los dispositivos administrados.

Antes de iniciar el Asistente de migración en Kaspersky Security Center Cloud Console, asegúrese de que el idioma de localización que esté utilizando sea el mismo que el que haya utilizado en Kaspersky Security Center Web Console durante el proceso de exportación. De no ser así, cambie el idioma.

Si antes de comenzar con este proceso utilizó el asistente de inicio rápido en su espacio de trabajo de Kaspersky Security Center Cloud Console, el grupo **Dispositivos administrados** contendrá directivas y tares con la configuración predeterminada. Elimínelas antes de importar las directivas y las tareas que exportó de Kaspersky Security Center Web Console.

Para importar el 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**. Cuando se abra la ventana del Explorador de archivos, vaya a la carpeta en la que haya guardado el archivo de exportación, selecciónelo y haga clic en **Abrir**. Espere a que el ícono de actualización (🔄) ubicado junto al estado de carga del archivo cambie por una marca de verificación verde (✓).

3. Haga clic en **Siguiente**. Se abre la siguiente página, en la que se muestra toda la jerarquía de grupos de administración del Servidor de administración de Kaspersky Security Center Cloud Console.

4. Active la casilla de verificación ubicada junto al grupo de administración en el que quiera restaurar los objetos de grupo y haga clic en **Siguiente**. El Asistente de migración le mostrará una lista con los paquetes de instalación del Agente de red disponibles en Kaspersky Security Center Cloud Console.

5. Seleccione el paquete de instalación que contenga la versión y localización del Agente de red que precise y haga clic en **Siguiente**.

Seleccione el paquete de instalación del Agente de red de Kaspersky para Windows solo si completó el asistente de inicio rápido en su espacio de trabajo de Kaspersky Security Center Cloud Console y si los dispositivos involucrados en la migración utilizan Windows.

Espere a que el Asistente de migración cree un paquete de instalación independiente. Existe un límite de tamaño de 200 MB para el paquete de instalación independiente del Agente de red.

El archivo se descomprimirá y se guardará automáticamente en la carpeta de descargas predeterminada del navegador. Los objetos de grupo y los que no estén vinculados a un grupo se restaurarán en el grupo de administración de destino.

Una vez que concluya la importación, verá la estructura de grupos de administración exportada (incluidos los detalles de los dispositivos) en el grupo de administración de destino que haya seleccionado. Si intenta restaurar un objeto que tenga el mismo nombre que un objeto existente, se agregará un sufijo secuencial al nombre del objeto restaurado.

Si importó el grupo **Dispositivos administrados** completo, recomendamos que cambie el nombre del subgrupo importado para evitar confusiones. Para ello, haga lo siguiente:

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**, escriba un nombre diferente (por ejemplo, "Dispositivos migrados").

Recomendamos verificar que los objetos incluidos en el alcance de la exportación (las directivas, las tareas y los dispositivos administrados) se hayan importado correctamente en Kaspersky Security Center Cloud Console. Para tal fin, diríjase a la sección **Activos (dispositivos)** y compruebe que los objetos importados aparezcan en las listas de 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 íconos de actualización (🔄) ubicados junto a los elementos de la lista de objetos cambien por marcas de verificación verdes (✓) y se complete la importación. Tras ello, los dispositivos comenzarán a quedar bajo el mando de Kaspersky Security Center Cloud Console.

6. Haga clic en **Finalizar** para completar el Asistente de migración.

7. Si desea buscar y descargar el paquete de instalación independiente de nuevo, vaya a **Descubrimiento 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 dispositivos diferentes, deberá copiar el paquete de instalación independiente en una unidad extraíble o elegir otra forma de transferir el archivo.

Paso 3. Reinstalar el Agente de red en los dispositivos administrados a través de Kaspersky Security Center Cloud Console

Tras crear el paquete de instalación independiente para el Agente de red, debe crear una tarea de instalación remota. Utilizará esta tarea para reinstalar el Agente de red en los dispositivos administrados y ceder el control de los mismos a Kaspersky Security Center Cloud Console.

Para reducir el riesgo de que se pierda información, recomendamos que primero realice estas acciones en un grupo de administración pequeño, que contenga no más de veinte dispositivos administrados de la red corporativa. Asegúrese de que el grupo 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 reinstalar el Agente de red:

1. Vuelva al Asistente de migración en la instancia local de Kaspersky Security Center Web Console.

   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.

   Dependiendo del estado en el que se encuentre el Asistente de migración, realice una de las siguientes acciones:

   - Si no cerró el Asistente de migración después de la exportación y su sesión sigue activa, haga clic en el botón **Ir al paso 3 del Asistente de migración**. Active la casilla de verificación **Cargar paquete de instalación independiente** y haga clic en el botón **Seleccionar un paquete de instalación independiente**. En la ventana que se abrirá en el navegador, seleccione el paquete de instalación independiente del Agente de red.

   - Si tiene que iniciar el Asistente de migración nuevamente, active la casilla de verificación **Cargar paquete de instalación independiente** y haga clic en el botón **Seleccionar un paquete de instalación independiente**. En la ventana que se abrirá en el navegador, seleccione el paquete de instalación independiente del Agente de red. Tras ello, el Asistente de migración mostrará nuevamente la jerarquía de grupos de administración de este Servidor de administración. Seleccione el mismo grupo para el que haya creado el archivo de exportación y haga clic en **Siguiente**.

     El Asistente de migración volverá a contar la cantidad de dispositivos administrados incluidos en el grupo de administración seleccionado. Si el número es superior a 10 000, verá un mensaje de error. No podrá hacer clic en el botón **Siguiente**, que estará atenuado, hasta que reduzca al máximo permitido (o menos) la cantidad de dispositivos administrados del grupo de administración seleccionado.

2. Espere a que se cargue el paquete de instalación independiente y haga clic en **Siguiente**. El Asistente de migración creará un paquete de instalación personalizado y una tarea de instalación remota para él. El alcance de la tarea incluirá el grupo de administración seleccionado en la página **Dispositivos administrados para exportar**; el horario de inicio de la tarea se establecerá, de forma predeterminada, en **Manual**. El Asistente de migración mostrará el avance del proceso de creación. Espere a que los íconos de actualización (🔄) cambien a marcas de verificación verdes (✓) y haga clic en **Siguiente**.

3. De ser necesario, active la casilla de verificación **Ejecutar la nueva tarea de instalación remota** (por defecto, se encuentra desactivada) para los dispositivos del grupo de administración seleccionado (y todos sus subgrupos) en el Servidor de administración local. En este caso, el control de los dispositivos pasará Kaspersky Security Center Cloud Console, pero solo después de que se complete la instalación del Agente de red. Se mostrará la ruta completa del grupo de administración en el que se realizará la tarea.

La tarea debe iniciarse solo después de que finalice la importación en Kaspersky Security Center Cloud Console. De lo contrario, los nombres de los dispositivos podrían aparecer dos veces 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:

   - Actualizar las instancias del Agente de red
   - Poner las instancias del Agente de red bajo el mando de Kaspersky Security Center Cloud Console

   Si ha dejado desactivada la casilla de verificación **Ejecutar la nueva tarea de instalación remota**, podrá iniciar la tarea manualmente más tarde, de ser necesario.

Puede comprobar que, ahora, las instancias del Agente de red migradas se administran a través de Kaspersky Security Center Cloud Console. Para ello, vaya a **Activos (dispositivos)** → **Dispositivos administrados**. Asegúrese de que los dispositivos administrados que migró tengan un ícono de confirmación (✓) en las columnas **Visible**, **Agente de red instalado** y **Agente de red en ejecución**. Verifique también que la descripción de estado de esos dispositivos no sea *Sin conexión desde hace mucho tiempo*.

Migración con una jerarquía de servidores de administración

En esta sección, se describe un método para migrar dispositivos administrados y objetos afines de un despliegue local de Kaspersky Security Center Web Console a Kaspersky Security Center Cloud Console. El proceso requiere que exista una jerarquía de servidores de administración. En esta jerarquía, la instancia local de Kaspersky Security Center Web Console debe actuar como Servidor de administración secundario, mientras que Kaspersky Security Center Cloud Console actuará como Servidor de administración principal.

Cada grupo de administración que transfiera a Kaspersky Security Center Cloud Console deberá contener dispositivos administrados que ejecuten un único sistema operativo. Si tiene dispositivos con diferentes sistemas operativos en su red, asígnelos a grupos de administración diferentes y migre cada grupo por separado.

Al concluir la migración, las copias del Agente de red instaladas en el grupo migrado se actualizarán y pasarán a ser controladas por 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 la versión 12.1 (o una posterior) de Kaspersky Security Center Web Console.
- Actualice el Agente de red en los dispositivos administrados a la versión 12 o una posterior.
- En los dispositivos con Windows, use el Agente de red sin contraseña de desinstalación.

  Si ya había definido esta contraseña, realice una de las siguientes acciones en Kaspersky Security Center Web Console:

  - Deshabilite la opción **Utilizar contraseña de desinstalación** en los ajustes de la directiva del Agente de red.

- Desinstale el Agente de red en forma remota con la tarea *Desinstalar aplicación de forma remota*. En el campo **Aplicación para desinstalar** de la tarea, seleccione **Agente de red de Kaspersky Security Center**. No olvide ingresar la contraseña de desinstalación.

- Actualice las aplicaciones administradas a versiones que sean 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 de las aplicaciones que planee 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 toda la información que Kaspersky Endpoint Security para Windows haya cifrado (a nivel de disco o de archivo) en los dispositivos con Windows administrados. Luego, deshabilite la función de cifrado en esos dispositivos (puede hacer esto en forma local o a través de la directiva de la aplicación). Para obtener más información, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

  Si durante el proceso de migración se detecta que un dispositivo con Windows aún tiene archivos o carpetas cifrados mediante Kaspersky Endpoint Security para Windows, se cancelará la actualización del Agente de red. A través de una notificación, se le pedirá que descifre todos los datos del dispositivo y que desactive la función de cifrado.

Kaspersky Security Center Cloud Console admite un máximo de 25 000 dispositivos administrados por Servidor de administración.

Para realizar la migración a Kaspersky Security Center Cloud Console, siga estos pasos:

1. Estime el alcance del proceso de migración, es decir, revise el grupo de administración que desee exportar y evalúe la cantidad de dispositivos administrados que contiene. Asegúrese de haber completado correctamente todas las actividades que figuran como requisitos previos para la migración.

2. En Kaspersky Security Center Cloud Console, vaya al Servidor de administración secundario correspondiente a los dispositivos administrados que desee 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**. Verá toda la jerarquía de grupos de administración del Servidor de administración secundario.

5. En la página **Dispositivos administrados para exportar**, haga clic en el ícono del corchete angular (>) ubicado junto al nombre del grupo **Dispositivos administrados**. A continuación, expanda la jerarquía de grupos de administración. Seleccione el grupo de administración que desee exportar.

El Asistente de migración contará la cantidad de dispositivos administrados incluidos en el grupo de administración seleccionado. Si el número es superior a 10 000, verá un mensaje de error. No podrá hacer clic en el botón **Siguiente**, que estará atenuado, hasta que reduzca al máximo permitido (o menos) la cantidad de dispositivos administrados del grupo de administración seleccionado.

6. Seleccione las aplicaciones administradas cuyas directivas y tareas quiera transferir a Kaspersky Security Center Cloud Console junto con los objetos del grupo. Para seleccionar las aplicaciones administradas a las que correspondan los objetos que quiera exportar, active las casillas de verificación adyacentes a los nombres de esas aplicaciones en la lista.

   Aunque el Servidor de administración de Kaspersky Security Center estará incluido en la lista, sus directivas no se exportarán si activa la casilla de verificación correspondiente.

   Para verificar si sus aplicaciones administradas son compatibles con Kaspersky Security Center Cloud Console, haga clic en el vínculo correspondiente. Se abrirá un tema de la Ayuda en línea con la lista de aplicaciones administradas por Kaspersky Security Center Cloud Console.

   Si selecciona aplicaciones incompatibles con Kaspersky Security Center Cloud Console, las directivas y las tareas de esas aplicaciones se migrarán de todos modos, pero no podrá administrarlas en Kaspersky Security Center Cloud Console porque no contará con los complementos dedicados que se requieren.

7. Revise la lista de objetos del grupo que se exportarán por defecto. 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. La 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 elige una tarea global asociada a una selección de objetos específica, también se exportará la selección.

     Aunque aparezcan en la lista, las tareas globales del Servidor de administración no se pueden exportar. Si selecciona estas tareas, el alcance de la exportación no cambiará. Las tareas de instalación remota también quedan excluidas 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**

Una lista editable con las instancias de los informes que se exportarán.

Si elige un informe asociado a una selección de objetos específica, también se exportará la selección.

Kaspersky Security Center Cloud Console contiene el mismo conjunto de plantillas de informes que Kaspersky Security Center Web Console. Por ello, al momento de elegir los informes para exportar, solamente podrá seleccionar aquellos que haya creado o reconfigurado manualmente.

- **Objetos de grupo**

La lista de objetos del grupo que se exportarán por defecto. De manera predeterminada, se exportarán en su totalidad los siguientes objetos relacionados con el grupo de administración seleccionado:

- 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 creó una etiqueta en Kaspersky Security Center Web Console, pero nunca la asignó a un dispositivo, no se la exportará. Las reglas de 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 exportarán.

- 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 exportarán.

También puede evitar que se exporten ciertos tipos de objetos no vinculados al grupo:

- Si no desea que se exporten los roles personalizados (es decir, aquellos creados por el usuario únicamente), active la casilla de verificación **Excluir roles personalizados de la exportación**.
- Si no desea que se exporten los usuarios internos ni los grupos de seguridad, active la casilla de verificación **Excluir usuarios internos y grupos de seguridad de la exportación**.
- Si no desea que se exporten las categorías de aplicaciones personalizadas con contenido agregado manualmente, active la casilla de verificación **Excluir categorías de aplicaciones personalizadas de la exportación**.

Si transfiere dispositivos con diferentes sistemas operativos a Kaspersky Security Center Cloud Console, solo tendrá que migrar los objetos que no estén vinculados a un grupo una vez.

8. Después de definir el alcance de la migración, haga clic en **Siguiente** para comenzar el proceso de exportación. Se abre la página **Creación del archivo de exportación**, en la que puede ver el progreso de exportación de cada tipo de objeto incluido en el alcance de la migración. Espere a que cada ícono de actualización (🔄) ubicado junto a los elementos de la lista de objetos cambie por una marca de verificación verde (✓). Cuando concluya la exportación, el archivo de exportación se guardará automáticamente en una carpeta temporal. Se abrirá la siguiente página, que muestra la jerarquía completa de los grupos de administración de Kaspersky Security Center Cloud Console, que actúa como el Servidor de administración principal.

9. Active la casilla de verificación ubicada junto al grupo de administración en el que deban importarse importar los objetos del grupo y haga clic en **Siguiente**. Se desempaqueta el archivo. Los objetos del grupo y los objetos que no están vinculados al grupo se restauran en el grupo de administración de destino.

   Si intenta restaurar un objeto que tenga el mismo nombre que un objeto existente, se agregará un sufijo secuencial al nombre del objeto restaurado.

   Una vez que concluya la importación, verá la estructura de grupos de administración exportada (incluidos los detalles de los dispositivos) en el grupo de administración de destino que haya seleccionado. Los objetos que no sean del grupo también se importarán.

   No podrá minimizar el Asistente de migración ni realizar ninguna operación simultánea durante la importación. Espere a que cada ícono de actualización (🔄) ubicado junto a los elementos de la lista de objetos cambie por una marca de verificación verde (✓) y se complete la importación. Tras ello, los dispositivos comenzarán a quedar bajo el mando de Kaspersky Security Center Cloud Console.

10. Una vez que finalice la importación, el Asistente de migración le mostrará una lista de los paquetes de instalación del Agente de red disponibles en Kaspersky Security Center Cloud Console para el sistema operativo pertinente. Seleccione el paquete de instalación que contenga la versión y localización del Agente de red que precise.

    Seleccione el paquete de instalación del Agente de red de Kaspersky para Windows solo si completó el asistente de inicio rápido en su espacio de trabajo de Kaspersky Security Center Cloud Console y si los dispositivos involucrados en la migración utilizan Windows.

11. Haga clic en **Siguiente**.

    El Asistente de migración creará un nuevo paquete de instalación independiente (o tomará uno existente) y lo utilizará de base para crear un paquete de instalación personalizado. El Asistente también creará la tarea de instalación remota correspondiente. El alcance de la tarea incluirá el grupo de administración seleccionado en la página **Dispositivos administrados para exportar**. De manera predeterminada, el horario de inicio de la tarea se fija en **Manual**. El Asistente de migración mostrará el avance del proceso de creación.

12. Espere a que cada ícono de actualización (🔄) cambie por una marca de verificación verde (✓) y haga clic en **Siguiente**.

13. De ser necesario, active la casilla de verificación **Ejecutar la nueva tarea de instalación remota** (desactivada de manera predeterminada) para los dispositivos del grupo de administración seleccionado (y todos sus subgrupos) en la instancia local de Kaspersky Security Center Web Console. Al concluir la instalación del Agente de red, podrá administrar los dispositivos seleccionados mediante Kaspersky Security Center Cloud Console. Verá la ruta completa del grupo de administración en el que se realizará la tarea.

La tarea de instalación remota debe iniciarse una vez que finaliza la importación en Kaspersky Security Center Cloud Console. De lo contrario, los dispositivos podrían duplicarse.

14. Haga clic en **Finalizar** para cerrar el Asistente de migración e iniciar la tarea de instalación remota para los siguientes propósitos:

    - Actualizar las instancias del Agente de red
    - Administrar las instancias del Agente de red mediante Kaspersky Security Center Cloud Console

    Si ha dejado desactivada la casilla de verificación **Ejecutar tarea de instalación remota**, podrá iniciar la tarea manualmente más tarde, de ser necesario.

Puede comprobar que, ahora, las instancias del Agente de red migradas se administran a través de Kaspersky Security Center Cloud Console. Para ello, vaya a **Activos (dispositivos)** → **Dispositivos administrados**. Asegúrese de que los dispositivos administrados que migró tengan un ícono de confirmación (✓) en las columnas **Visible**, **Agente de red instalado** y **Agente de red en ejecución**. Verifique también que la descripción de estado de esos dispositivos no sea *Sin conexión desde hace mucho tiempo*.

Escenario: Migración de dispositivos con sistemas operativos Linux o macOS

En esta sección, se describe el proceso para migrar dispositivos con Linux o macOS de un despliegue local de Kaspersky Security Center Web Console a Kaspersky Security Center Cloud Console. Puede completar los escenarios básicos para realizar una migración sin una jerarquía o con una jerarquía de servidores de administración y transferir la totalidad de sus dispositivos y objetos relacionados a Kaspersky Security Center Cloud Console. Sin embargo, si no solo tiene dispositivos con Windows en su red, sino también dispositivos con Linux o macOS, deberá transferir los dispositivos con cada sistema operativo por separado. En consecuencia, deberá llevar a cabo la migración varias veces.

Requisitos previos

Antes de comenzar, haga lo siguiente:

- Actualice el Servidor de administración local a la versión 12 parche A o a una versión posterior.
- Instale la versión 12.1 (o una posterior) de Kaspersky Security Center Web Console.
- Actualice el Agente de red en los dispositivos administrados a la versión 12 o a una posterior.
- Actualice las aplicaciones administradas a versiones que sean 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 de las aplicaciones que planee 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 admite un máximo de 25 000 dispositivos administrados por Servidor de administración.

Etapas de la migración

La migración a Kaspersky Security Center Cloud Console se divide en las siguientes etapas:

1. **Agrupar los dispositivos administrados por sistema operativo**

   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. Cree también un grupo de administración para cada distribución de Linux. Si tiene dispositivos con Debian y Red Hat, por ejemplo, colóquelos en grupos de administración diferentes. Esto es necesario para que la migración se complete correctamente, ya que cada sistema operativo necesita un paquete de instalación diferente para el Agente de red.

2. **Migrar cada grupo de administración y sus objetos de aplicación por separado**

   Para que se incluyan sus directivas y tareas, los dispositivos con sistemas operativos diferentes se deben migrar por separado. Por ejemplo, si necesita transferir dispositivos con Windows, macOS, Ubuntu y CentOS a Kaspersky Security Center Cloud Console, transfiera primero los dispositivos con Windows, luego los dispositivos con macOS, luego los que tengan Ubuntu y, por último, los dispositivos con CentOS. Puede transferir los dispositivos administrados en cualquier orden.

   La migración puede realizarse sin una jerarquía o con una jerarquía de servidores de administración; la elección dependerá de si tiene servidores de administración secundarios en su red. Durante la migración, utilice el paquete de instalación del Agente de red correspondiente al sistema operativo de los dispositivos transferidos. Por ejemplo, para realizar la migración de manera correcta, seleccione el Agente de red de Kaspersky Security Center 13.2 para dispositivos Linux.

   Tenga en cuenta que los objetos que no están vinculados a un grupo, como las tareas globales, los informes y las selecciones de dispositivos personalizadas, solo necesitan migrarse una vez.

Resultados

Al finalizar la migración, puede asegurarse de que el proceso se haya realizado correctamente. Para ello, verifique lo siguiente:

- Se reinstaló la versión adecuada del Agente de red en cada dispositivo administrado con sistema operativo Linux o macOS.
- Todos los dispositivos con Linux o macOS quedaron bajo la órbita administrativa de Kaspersky Security Center Cloud Console.
- Se conservaron todos los ajustes que estaban en vigencia antes de la migración.

Escenario: Migración inversa de Kaspersky Security Center Cloud Console a Kaspersky Security Center

En algunos casos, querrá migrar sus dispositivos administrados de Kaspersky Security Center Cloud Console a un Servidor de administración de Kaspersky Security Center. Podría utilizar este proceso, por ejemplo, para revertir una 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 para el Agente de red en el Servidor de administración local de Kaspersky Security Center**

   En el Servidor de administración local de Kaspersky Security Center, cree un paquete de instalación independiente para el Agente de red.

   Durante el proceso de creación, puede habilitar la opción **Mover los dispositivos no asignados a este grupo** y seleccionar el grupo de administración al que se moverán las instancias del Agente de red cuando se complete 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 evitar inconvenientes al realizar la migración inversa, la versión del Agente de red debe ser la misma o más reciente que la que utiliza en Kaspersky Security Center Cloud Console.

2. **Crear un paquete de instalación personalizado 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 en la instancia local del Servidor de administración de Kaspersky Security Center.

   Para que el paquete se instale en modo silencioso, en el campo **Línea de comandos para el archivo ejecutable**, introduzca la clave `-s`.

3. **Crear 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. **Ejecutar la tarea de instalación remota**

Inicie la tarea de instalación remota que creó en el paso anterior. La tarea hará que todas las instancias del Agente de red se reinstalen en el grupo de administración seleccionado. Asimismo, se cederá el control de esas instancias al Servidor de administración local de Kaspersky Security Center. Para tal fin, la tarea modificará la dirección de conexión y otros ajustes afines.

Si no eligió un grupo de administración de destino al crear el paquete de instalación independiente, todos los dispositivos se moverán al grupo **Dispositivos no asignados**.

Resultados

Al finalizar la migración, puede asegurarse de que el proceso se haya realizado correctamente. Para ello, verifique lo siguiente:

- Los dispositivos incluidos el alcance de la tarea de instalación remota que antes se administraban mediante Kaspersky Security Center Cloud Console ahora se administran por medio del Servidor de administración local de Kaspersky Security Center.
- Los dispositivos se movieron automáticamente al grupo de administración indicado en la configuración del paquete de instalación.

La tarea de instalación remota no se podrá completar en Kaspersky Security Center Cloud Console: se quedará sin dispositivos de destino, ya que los ajustes de conexión se habrán modificado en cada dispositivo. Deberá detener la tarea manualmente tras verificar que, en la lista de dispositivos administrados, todos los dispositivos incluidos en el alcance de la migración tengan el ícono de error (!) en la columna **Visible**.

Migración con servidores de administración virtuales

Si tiene servidores de administración virtuales en su infraestructura local de Kaspersky Security Center, no podrá utilizar el Asistente de migración para realizar la migración de Kaspersky Security Center local a Kaspersky Security Center Cloud Console. Además, solo podrá migrar los dispositivos de sus clientes. Deberá crear directivas, tareas e informes manualmente.

Puede realizar uno de los siguientes escenarios de migración:

- Trasladando los dispositivos de sus clientes de los servidores de administración virtuales a un Servidor de administración principal.
- Realizar una migración manual desde los Servidores de administración virtuales.

Escenario: Migración con Servidores de administración virtuales al mover dispositivos

Para realizar la migración de Kaspersky Security Center Web Console que se ejecuta de forma local 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, actualizar el Servidor de administración local a la versión 12 (o posterior) y actualizar las aplicaciones administradas a versiones que sean compatibles con Kaspersky Security Center Cloud Console.

Escenario de migración

El escenario se divide en etapas:

1. **Crear un grupo de administración para cada Servidor de administración virtual**

   Puede crear estos grupos en su instancia local de Kaspersky Security Center.

2. **Trasladar los dispositivos de los clientes**

   En la instancia local de Kaspersky Security Center, mueva los dispositivos de sus clientes de cada Servidor de administración virtual al grupo de administración respectivo creado en la etapa anterior.

3. **Realizar la migración**

   Realice la migración siguiendo las instrucciones para una red sin una jerarquía de Servidores de administración.

4. **Ceder el control de los dispositivos a servidores de administración virtuales (paso opcional)**

   Si desea utilizar de servidores de administración virtuales para administrar a sus clientes, ceda a esos servidores el control de los dispositivos que se encuentran en los grupos de administración.

5. **Crear directivas, tareas e informes**

   Cree las directivas, las tareas y los informes que se precisen.

Resultados

Al finalizar la migración, puede asegurarse de que el proceso se haya realizado correctamente. Para ello, verifique lo siguiente:

- 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 conservaron todos los ajustes que estaban en vigencia 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 de manera manual.

Requisitos previos

Antes de la migración, debe realizar una serie de acciones, entre ellas, actualizar el Servidor de administración local a la versión 12 (o posterior) y actualizar las aplicaciones administradas a versiones que sean compatibles con Kaspersky Security Center Cloud Console.

Escenario de migración

El escenario se divide en etapas:

1. **Crear un grupo de administración para cada Servidor de administración virtual**

   En Kaspersky Security Center Cloud Console, cree un grupo de administración que corresponda a cada uno de sus servidores de administración virtuales.

2. **Crear un paquete de instalación independiente para el Agente de red**

   Cree un paquete de instalación independiente para el Agente de red. Durante el proceso de creación, especifique un grupo de administración creado en la etapa anterior. Deberá crear un paquete de instalación independiente para cada grupo de administración.

   Las acciones de esta etapa deben realizarse en Kaspersky Security Center Cloud Console.

3. **Descargar los paquetes de instalación independientes**

   Descargue los paquetes de instalación independientes que ha creado en la etapa anterior. Las acciones de esta etapa deben realizarse en Kaspersky Security Center Cloud Console.

4. **Crear un archivo de almacenamiento con cada paquete de instalación independiente**

   Los tipos de archivo disponibles son ZIP, CAB, TAR y TAR.GZ.

5. **Crear paquetes de instalación personalizados para el Agente de red**

   Cree paquetes de instalación personalizados para el Agente de red. Para crear estos paquetes, utilice los archivos de almacenamiento que creó en la etapa anterior.

   Las acciones de esta etapa deben realizarse en la instancia local de Kaspersky Security Center.

6. **Crear tareas de instalación remota**

   Cree tareas de instalación remota para instalar el Agente de red utilizando los paquetes de instalación personalizados que creó en la etapa anterior.

   Cuando esté creando cada tarea, especifique el grupo de administración correspondiente.

   Las acciones de esta etapa deben realizarse en la instancia local de Kaspersky Security Center.

7. **Ejecutar las tareas de instalación remota**

   Las instancias del Agente de red se actualizarán. El Servidor de administración de Kaspersky Security Center Cloud Console se hará cargo de administrarlos.

   Todos los dispositivos migrarán a Kaspersky Security Center Cloud Console. Se los agregará a los grupos de administración que haya indicado al crear los paquetes de instalación independientes para el Agente de red.

8. **Ceder el control de los dispositivos a servidores de administración virtuales (paso opcional)**

   Si desea utilizar de servidores de administración virtuales para administrar a sus clientes, ceda a esos servidores el control de los dispositivos que se encuentran en los grupos de administración.

9. **Crear directivas, tareas e informes**

   Cree las directivas, las tareas y los informes que se precisen.

Resultados

Al finalizar la migración, puede asegurarse de que el proceso se haya realizado correctamente. Para ello, verifique lo siguiente:

- 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 conservaron todos los ajustes que estaban en vigencia antes de la migración.

Escenario: Mover dispositivos desde los grupos de administración bajo la administración de Servidores virtuales

Posiblemente quiera utilizar servidores de administración virtuales para administrar a sus clientes. Si ha migrado los dispositivos (y otros elementos) de sus clientes de un despliegue local de Kaspersky Security Center a Kaspersky Security Center Cloud Console, los dispositivos migrados se encontrarán en grupos de administración. Para administrar esos dispositivos a través de servidores de administración virtuales, deberá ceder el control de los dispositivos a los servidores de administración virtuales.

Requisitos previos

Debe haber creado un Servidor de administración virtual para cada cliente.

Los dispositivos de cada cliente deben estar en un grupo de administración individual.

Etapas

El escenario se divide en etapas:

1. **Crear 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 de Servidor de administración, puede utilizar el menú principal: haga clic en el ícono del corchete angular (›) a la derecha del nombre del Servidor de administración con el que esté trabajando y, luego, seleccione el Servidor de administración con el que quiera operar.

2. **Descargar los paquetes de instalación independientes**

   Descargue los paquetes de instalación independientes que ha creado en la etapa anterior.

3. **Crear un archivo de almacenamiento con cada paquete de instalación independiente**

   Los tipos de archivo disponibles son ZIP, CAB, TAR y TAR.GZ.

4. **Crear paquetes de instalación personalizados para el Agente de red**

   Cree paquetes de instalación personalizados para el Agente de red. Para crear estos paquetes, utilice los archivos de almacenamiento que creó en la etapa anterior.

   Esta etapa se desarrolla en el Servidor de administración principal.

5. **Crear tareas de instalación remota**

   Cree tareas de instalación remota para instalar el Agente de red utilizando los paquetes de instalación personalizados que creó en la etapa anterior.

   Cuando esté creando cada tarea, especifique el grupo de administración correspondiente.

   Esta etapa se desarrolla en el Servidor de administración principal.

6. **Ejecutar las tareas de instalación remota**

   Las instancias del Agente de red se actualizarán. El control de los dispositivos administrados pasará a los servidores de administración virtuales.

7. **Crear directivas, tareas e informes**

   Cree las directivas, las tareas y los informes que se precisen.

Resultados

Ahora puede administrar los dispositivos de los clientes migrados mediante Servidores de administración virtuales.

Acerca de la migración desde Pro View a Expert View

La migración solo está disponible si tiene una licencia de Kaspersky Next.

Para obtener una descripción detallada del procedimiento de migración, consulte la Ayuda de Kaspersky Endpoint Security Cloud.

Una vez finalizada la migración, se crea un nuevo espacio de trabajo en Expert View y recibe la notificación correspondiente por correo electrónico. 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:

- 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 se muestran en la lista de dispositivos administrados.

  Los dispositivos transferidos se conectan automáticamente al espacio de trabajo creado en Expert View. Esto puede llevar unos minutos.

- En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.

  En la lista de directivas, se muestra la directiva del Agente de red con la protección con contraseña configurada.

Asistente de inicio rápido

En esta sección, encontrará información sobre el asistente de inicio rápido de Kaspersky Security Center Cloud Console.

Acerca del asistente de inicio rápido

El asistente de inicio rápido de Kaspersky Security Center Cloud Console le permite crear una serie de tareas y directivas que se consideran indispensables, configurar los ajustes básicos y comenzar a crear paquetes de instalación para las aplicaciones de Kaspersky. Puede usar el asistente para realizar los siguientes cambios en Kaspersky Security Center Cloud Console:

- Iniciar la descarga de paquetes de instalación para las aplicaciones de Kaspersky administradas.
- Crear un paquete de instalación independiente para instalar el Agente de red en dispositivos con Windows, Linux o macOS.
- Crear una directiva para el Agente de red de Kaspersky Security Center.
- Cree la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*.
- Crear directivas y tareas para las aplicaciones de Kaspersky administradas.
- Configurar la interacción con Kaspersky Security Network (KSN).

Una vez que termine de usar el asistente de inicio rápido, encontrará los paquetes de instalación para el Agente de red y las aplicaciones de Kaspersky administradas en la lista **Descubrimiento y despliegue → Despliegue y asignación → Paquetes de instalación**.

El asistente de inicio rápido creará directivas para las aplicaciones administradas, como Kaspersky Endpoint Security para Windows, siempre y cuando el grupo "Dispositivos administrados" no contenga aún tales directivas. El asistente de inicio rápido creará las tareas siempre y cuando no existan otras con el mismo nombre para el grupo "Dispositivos administrados".

Kaspersky Security Center Cloud Console le pedirá automáticamente que ejecute el asistente de inicio rápido luego de que cree un espacio de trabajo para su empresa e inicie Kaspersky Security Center Cloud Console por primera vez. El asistente de inicio rápido también se puede ejecutar manualmente en cualquier momento.

Ejecución del asistente de inicio rápido

Kaspersky Security Center Cloud Console le pedirá automáticamente que ejecute el asistente de inicio rápido luego de que cree un espacio de trabajo para su empresa e inicie Kaspersky Security Center Cloud Console por primera vez. El asistente de inicio rápido también se puede ejecutar manualmente en cualquier momento.

Si inicia el asistente de inicio rápido una segunda vez, no se volverán a crear las tareas y directivas que haya creado en la ejecución anterior.

Para iniciar el asistente de inicio rápido manualmente:

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

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **General**.

3. Haga clic en **Iniciar el Asistente de inicio rápido**.

   Como alternativa, para iniciar el asistente de inicio rápido, haga clic en **Descubrimiento y despliegue** → **Despliegue y asignación** → **Asistente de inicio rápido**.

El asistente le pedirá que realice la configuración inicial de Kaspersky Security Center Cloud Console. Siga las instrucciones del asistente. Avance por el asistente utilizando el botón **Siguiente**. Utilice el botón **Atrás** para volver al paso anterior del asistente.

Paso 1. Selección de los paquetes de instalación que se van a descargar

En la lista, seleccione las aplicaciones de Kaspersky que desee instalar en los dispositivos cliente. Kaspersky Security Center Cloud Console creará paquetes de instalación para las aplicaciones seleccionadas. Usted usará luego esos paquetes de instalación para instalar las aplicaciones.

Cuando seleccione 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 instalarse en todos los dispositivos cliente. Por lo tanto, seleccione un Agente de red apropiado para el sistema operativo de cada dispositivo cliente.

  - Deberá instalar el Agente de red manualmente, utilizando un paquete de instalación independiente, en el dispositivo que designe como punto de distribución. Los puntos de distribución se necesitan para realizar sondeos en la red e instalar las aplicaciones de seguridad de Kaspersky de manera remota en los dispositivos cliente. Seleccione, por ende, al menos un paquete de instalación del Agente de red. Kaspersky Security Center Cloud Console creará un paquete de instalación independiente para el Agente de red mientras usted continúa con los pasos siguientes del asistente.

    Los puntos de distribución basados en Linux y macOS tienen limitaciones funcionales respecto de los puntos de distribución basados en Windows. Recomendamos que los dispositivos designados como puntos de distribución utilicen el sistema operativo Windows.

    Puede seleccionar versiones del Agente de red para Windows, Linux y macOS. Si selecciona un Agente de red para un único sistema operativo (por ejemplo, macOS), se creará un paquete de instalación independiente para el sistema operativo seleccionado. Si selecciona versiones del Agente de red para varios sistemas operativos, Kaspersky Security Center Cloud Console creará un único paquete de instalación independiente siguiendo este orden de prioridad: Windows tendrá la máxima prioridad, luego vendrá Linux y, finalmente, vendrá macOS. Si selecciona las versiones del Agente de red para Linux y macOS, por ejemplo, Kaspersky Security Center Cloud Console creará 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.

- Las 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. Los valores configurados se agregarán al paquete de instalación del Agente de red. Después de la instalación, el Agente de red usará automáticamente esos valores en cada dispositivo cliente.

Especifique los valores de los siguientes ajustes de conexión del 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 forma 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 descargó el paquete de instalación de Kaspersky Endpoint Security para Windows en el primer paso del asistente, se mostrará 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 mostrará la Declaración de KSN para esa 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 utilizar Kaspersky Security Network**

  Kaspersky Security Center Cloud Console y las aplicaciones administradas de los dispositivos cliente transferirán información sobre sus operaciones a Kaspersky Security Network de manera automática. Participar en Kaspersky Security Network permite que las bases de datos con información sobre virus y otros riesgos se actualicen más rápidamente, lo cual se traduce en una mayor velocidad de respuesta ante amenazas a la seguridad emergentes.

- **No acepto utilizar Kaspersky Security Network**

  Kaspersky Security Center 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 deshabilitado. Más adelante, si cambia de opinión sobre el uso de KSN, puede habilitar (o deshabilitar) 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 ya existe la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

Puede usar la opción **Buscar reparaciones de vulnerabilidades y actualizaciones de software de terceros** para obtener una lista de las vulnerabilidades presentes en las aplicaciones de los dispositivos administrados y una lista de las actualizaciones y parches que pueden usarse para reparar esas vulnerabilidades. Si habilita esta opción, Kaspersky Security Center Cloud Console creará 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 realizará dos operaciones:

- Crea directivas y tareas básicas con su configuración predeterminada

  Se crearán las siguientes directivas:

  - Directiva del Agente de red de Kaspersky Security Center
  - Directivas para las aplicaciones de Kaspersky administradas

Se crearán las siguientes tareas:

- La tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*
- La tarea *Buscar vulnerabilidades y actualizaciones requeridas*

  Esta tarea únicamente se creará si habilitó la opción **Buscar reparaciones de vulnerabilidades y actualizaciones de software de terceros** en el paso anterior del asistente.
- Tareas para las aplicaciones de Kaspersky administradas

- Crear un paquete de instalación independiente para el Agente de red

  Utilizará este paquete para instalar el Agente de red en los puntos de distribución. Para crear el paquete de instalación independiente, Kaspersky Security Center Cloud Console tomará como base el paquete de instalación del Agente de red seleccionado en el paso anterior del asistente. Durante la creación del paquete, se le pedirá que lea y acepte los términos del EULA para el Agente de red. Una vez que se cree el paquete de instalación independiente, se le solicitará que lo descargue al dispositivo que esté utilizando.

  La creación del paquete de instalación independiente para el Agente de red puede llevar unos momentos. Puede continuar con el siguiente paso del asistente. El proceso continuará en segundo plano. Si es necesario, puede realizar un seguimiento del estado de descarga del paquete de instalación en la columna **Estado del paquete** (**Descubrimiento 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 reemite de tanto en tanto. Cada vez que esto sucede, Kaspersky Security Center Cloud Console actualiza automáticamente la firma de los paquetes de instalación independientes que se crearon. Sin embargo, la firma de un paquete de instalación independiente que se ha descargado no se puede actualizar en forma automática. Debido a ello, si intenta instalar una aplicación utilizando un paquete de instalación independiente con un certificado caducado, podría ver un error relativo al certificado. Para solucionar este problema, vuelva a descargar el paquete de instalación independiente.

Paso 6. Cierre del asistente de inicio rápido

En la página de finalización del asistente de inicio rápido, lea sobre las operaciones adicionales que deberá llevar a cabo para desplegar las aplicaciones de seguridad de Kaspersky en los dispositivos cliente. Complete las etapas del escenario Despliegue inicial de las aplicaciones de Kaspersky.

Despliegue inicial de las aplicaciones de Kaspersky

En esta sección, se aborda el despliegue inicial de las aplicaciones de Kaspersky en los dispositivos cliente de su organización.

Escenario: Despliegue inicial de las aplicaciones de Kaspersky

En este escenario, se describe cómo utilizar Kaspersky Security Center Cloud Console para instalar las aplicaciones de Kaspersky en los dispositivos cliente de una red. El primer paso consiste en desplegar puntos de distribución en la red. Esos puntos de distribución se usan luego para sondear la red y descubrir los dispositivos conectados a la misma. Completado este proceso, se procede a desplegar las aplicaciones de Kaspersky en los dispositivos de la red.

Al concluir este escenario, habrá instalado las aplicaciones de Kaspersky en los dispositivos cliente que haya seleccionado dentro de la red de su organización. Podrá administrar todos los dispositivos que cuenten con aplicaciones de Kaspersky.

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 para el Agente de red y las aplicaciones de seguridad.
- La dirección https://aes.s.kaspersky-labs.com/endpoints/ está incluida en las excepciones del firewall de los dispositivos administrados.
- Ha tomado nota de los ajustes de Internet de los dispositivos cliente de la organización. Conoce asimismo los ajustes del servidor proxy y tiene información sobre la puerta de enlace.
- Los dispositivos cliente de su organización no están cifrados.

Etapas

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

1. **Seleccionar un dispositivo para que actúe como punto de distribución**

   En Kaspersky Security Center Cloud Console, un punto de distribución está destinado a:

   - permiten realizar sondeos de red y descubrir dispositivos;
   - permiten instalar el Agente de red en los dispositivos cliente de manera remota;
   - cuando actúan como puerta de enlace de conexión, permiten que los dispositivos cliente se conecten al Servidor de administración.

   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 **Crear 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 **Instalar el Agente de red en el dispositivo seleccionado como punto de distribución**

Copie el paquete de instalación independiente del Agente de red al dispositivo seleccionado. Utilice para ello cualquier método que considere apropiado. Podría, por ejemplo, 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.

En el dispositivo seleccionado, dé inicio a la instalación del paquete de instalación independiente del Agente de red. El Agente de red se instalará con la configuración indicada en el paquete de instalación del Agente de red y se conectará 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 trata de instalar el Agente de red con un paquete de instalación independiente en un dispositivo con Microsoft Windows XP Professional para sistemas integrados de 32 bits, no podrá terminar la instalación. 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 **Designar el dispositivo con el Agente de red como punto de distribución**

Designe el dispositivo en el que acaba de instalar el Agente de red como punto de distribución.

5 **Configure y realice sondeos de red con el punto de distribución**

Configure las opciones de sondeo de red para el punto de distribución con el Agente de red instalado. Como alternativa, 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 de Kaspersky administradas**

Si no utilizó el asistente de inicio rápido o si omitió el paso de creación de 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 **Eliminar 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 **Instalar las aplicaciones de Kaspersky en los 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 de forma remota** Para la tarea de instalar el Agente de red, use la opción **Con los recursos del sistema operativo a través de los puntos de distribución**. Para la tarea de instalar aplicaciones administradas de Kaspersky, use la opción **Con el Agente de red**. Tras crear las tareas, puede configurar sus ajustes. Asegúrese de que la programación de cada tarea sea acorde a sus necesidades. La primera tarea de instalación en ejecutarse debe ser la del Agente de red. La tarea para instalar las aplicaciones de Kaspersky se debe ejecutar una vez que el Agente de red se ha instalado en los dispositivos cliente.

Opcionalmente, puede crear una tarea de instalación remota para instalar el Agente de red y las aplicaciones de Kaspersky administradas en los dispositivos cliente conectados a la red de su organización. En este caso, en el bloque **Paquetes de instalación**, use la opción **Seleccione el paquete de instalación** y la opción **Seleccione el Agente de red**. En el bloque **Forzar la descarga del paquete de instalación**, use la opción **Con los recursos del sistema operativo a través de los 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, computadoras 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 de forma local en esos dispositivos cliente. Hecho esto, podrá instalar las aplicaciones de Kaspersky en los dispositivos de los usuarios remotos como lo haría en cualquier otro dispositivo descubierto 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 para Android.

10. **Verificar el 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.

En lo que respecta al cifrado de disco completo, Kaspersky Security Center Cloud Console solo es compatible con BitLocker.

Crear paquetes de instalación para las aplicaciones de Kaspersky

Si quiere desplegar las aplicaciones de Kaspersky en los dispositivos conectados a la red de su organización, debe crear paquetes de instalación para las mismas en Kaspersky Security Center Cloud Console.

Para crear un paquete de instalación para una aplicación de Kaspersky:

1. Realice una de las siguientes acciones:

   - En el menú principal, vaya a **Descubrimiento y despliegue → Despliegue y asignación → Paquetes de instalación**.
   - En el menú principal, vaya a **Operaciones → Repositorios → Paquetes de instalación**.

   Como alternativa, puede ver las notificaciones sobre nuevos paquetes que aparecen 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 con los paquetes de instalación disponibles en el Servidor de administración.

2. Haga clic en **Agregar**.

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

3. Seleccione **Crear un paquete de instalación para una aplicación de Kaspersky**.

   Aparece una lista con los 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 abre 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 el paquete de distribución no puede convertirse en paquete de instalación automáticamente, verá el botón **Descargar paquete de distribución** en lugar del botón **Descargar y crear paquete de instalación**. En ese caso, descargue el paquete de distribución y 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 el modo de segundo plano. Puede seguir el estado de descarga del paquete de instalación, además de 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 forma predeterminada, los paquetes de instalación con estados **En curso** y **Aceptar EULA** se colocan al principio de la lista.

   Si tiene pensado migrar de Kaspersky Security Center Web Console a Kaspersky Security Center Cloud Console y las normas de seguridad de su organización requieren utilizar un proxy al acceder a la red corporativa, el proceso de migración podría verse afectado. Tras crear un paquete de instalación para el Agente de red, deberá especificar los parámetros del proxy para garantizar la conexión entre las instancias del Agente de red de los dispositivos administrados y el espacio de trabajo de Kaspersky Security Center Cloud Console. Para tal fin, haga lo siguiente:

   a. Haga clic en el nombre del paquete de instalación.

   b. En la ventana que se abre, que contendrá las propiedades del paquete de instalación, 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 EULA**. Si ve este botón, haga lo siguiente:

   a. Haga clic en el botón **Mostrar EULA** para leer el Contrato de licencia de usuario final (EULA).

   b. Lea el EULA que aparece en pantalla y haga clic en el botón **Aceptar**.

      Una vez que acepte el EULA, la descarga continuará. Si hace clic en **Rechazar**, la descarga se detiene.

7. Cuando termine la descarga, haga clic en el botón **Cerrar** (×) para cerrar la ventana con información sobre el paquete de distribución.

Se creará el paquete de instalación. Lo encontrará 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**. De ser necesario, en el campo **Nombre de la tarea**, cambie el nombre predeterminado de la tarea.

   En el paso siguiente, especifique los servidores de administración secundarios que estarán alcanzados por la tarea y siga las instrucciones del Asistente para crear nueva tarea. El Asistente para crear nueva tarea creará la tarea para distribuir los paquetes de instalación seleccionados a esos servidores de administración secundarios específicos.

   > Cuando se crea una tarea "Distribuir paquete de instalación" para servidores de administración secundarios desplegados en una infraestructura local, el alcance de la distribución —dejando de lado los paquetes de instalación personalizados e independientemente de la opción de distribución que se haya seleccionado (**Todos los paquetes de instalación** o **Paquetes de instalación seleccionados**) — queda limitado a los paquetes de instalación de las aplicaciones de Kaspersky que son compatibles con un despliegue local de Kaspersky Security Center Web Console.

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 las personas que utilizan los dispositivos de su organización pueden usar paquetes de instalación independientes para instalar el Agente de red de manera local en los dispositivos. Puede crear paquetes de instalación independientes para dispositivos con Windows, Linux y macOS.

> Kaspersky Security Center Cloud Console solamente permite crear paquetes de instalación independientes 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 algún otro modo. El archivo recibido se puede ejecutar localmente en el dispositivo cliente para instalar el Agente de red sin involucrar a Kaspersky Security Center Cloud Console.

En el caso del Agente de red para Linux y para macOS, el paquete de instalación independiente es un archivo de script con la extensión ".sh". Cuando se ejecuta este archivo, el script desempaqueta un archivo adjunto que contiene el paquete de instalación y su configuración, y luego inicia la instalación.

Si trata de instalar el Agente de red con un paquete de instalación independiente en un dispositivo con Microsoft Windows XP Professional para sistemas integrados de 32 bits, no podrá terminar la instalación. 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 reemite de tanto en tanto. Cada vez que esto sucede, Kaspersky Security Center Cloud Console actualiza automáticamente la firma de los paquetes de instalación independientes que se crearon. Sin embargo, la firma de un paquete de instalación independiente que se ha descargado no se puede actualizar en forma automática. Debido a ello, si intenta instalar una aplicación utilizando un paquete de instalación independiente con un certificado caducado, podría ver un error relativo al certificado. Para solucionar este problema, 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 **Descubrimiento y despliegue → Despliegue y asignación → Paquetes de instalación**.
   - En el menú principal, vaya a **Operaciones → Repositorios → Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación. Si el paquete de instalación del Agente de red no está en la lista, créelo manualmente.

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 (de ser necesario) y cierre la ventana de propiedades del paquete.

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 **Usar un paquete independiente**.

   Se inicia el asistente de creación de paquetes de instalación independiente. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

6. Cerciórese de que la opción Instalar el **Instalar el Agente de red junto con esta aplicación** esté activada si desea instalar el Agente de red junto con la aplicación seleccionada.

   Esta opción está activada de forma predeterminada. Recomendamos que habilite 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, cuando se instale el paquete de instalación independiente, el Agente de red se actualizará a la versión más reciente.

   Si deshabilita esta opción, el Agente de red no se instalará en el dispositivo, y el dispositivo quedará como dispositivo no administrado.

El asistente le indicará si el Servidor de administración ya cuenta con un paquete de instalación independiente para la aplicación seleccionada. Si esto sucede, elija una de estas acciones:

- **Crear un paquete de instalación independiente**. Seleccione esta opción si, por ejemplo, desea crear un paquete de instalación independiente para una nueva versión de la aplicación y, al mismo tiempo, quiere conservar un paquete de instalación independiente creado para una versión más antigua de la aplicación. El nuevo paquete de instalación independiente se ubicará en otra carpeta.

- **Utilizar un paquete de instalación independiente que ya existe**. Seleccione esta opción si desea utilizar un paquete de instalación independiente que ya exista. El proceso para crear paquetes no se iniciará.

- **Volver a generar un paquete de instalación independiente que ya existe**. Seleccione esta opción si desea volver a crear un paquete de instalación independiente para la misma aplicación. El paquete de instalación independiente se ubicará en la misma carpeta.

7. En el paso **Mover a lista de dispositivos administrados**, la opción **No mover los dispositivos** se selecciona de manera predeterminada. Si no desea que el dispositivo cliente se mueva a un grupo de administración después de la instalación del Agente de red, deje seleccionada esta opción.

   Si desea que el dispositivo cliente se mueva después de la instalación del Agente de red, seleccione la opción **Mover los dispositivos no asignados a este grupo** y seleccione el grupo de administración al que desee 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 de creación de un paquete de instalación independiente.

Se crea el paquete de instalación independiente para el 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 **Descubrimiento y despliegue → Despliegue y asignación → Paquetes de instalación**.

   - En el menú principal, vaya a **Operaciones → Repositorios → Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación.

2. Haga clic en el botón **Ver la lista de paquetes independientes**, ubicado encima de la lista.

Se muestra una lista 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 del 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.
- **Hash de archivo**. Propiedad que permite certificar que el paquete de instalación independiente no ha sido modificado por ningún tercero y que el usuario tiene el mismo archivo que usted creó y le transfirió.

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 reemite de tanto en tanto. Cada vez que esto sucede, Kaspersky Security Center Cloud Console actualiza automáticamente la firma de los paquetes de instalación independientes que se crearon. Sin embargo, la firma de un paquete de instalación independiente que se ha descargado no se puede actualizar en forma automática. Debido a ello, si intenta instalar una aplicación utilizando un paquete de instalación independiente con un certificado caducado, podría ver un error relativo al certificado. Para solucionar este problema, 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 un paquete de instalación personalizado para estos fines:

- Para instalar cualquier aplicación (como un editor de texto) en un dispositivo cliente vinculado a Kaspersky Security Center Cloud Console, por ejemplo, mediante una tarea.
- Para crear un paquete de instalación independiente.

Un paquete de instalación personalizado es una carpeta que contiene un archivo ejecutable y otros archivos adicionales. La base para crear este paquete puede ser un archivo de almacenamiento. Dicho archivo debe contener uno o más de los archivos que formarán parte del paquete de instalación personalizado. Al crear un paquete de instalación personalizado, pueden agregarse parámetros de línea de comandos que hagan que, por ejemplo, la instalación se lleve a cabo 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 **Descubrimiento y despliegue → Despliegue y asignación → Paquetes de instalación**.
   - En el menú principal, vaya a **Operaciones → Repositorios → Paquetes de instalación**.

   Se muestra una lista con los paquetes de instalación disponibles en el Servidor de administración.

2. Haga clic en **Agregar**.

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

3. Seleccione **Crear un paquete de instalación a partir de un archivo**.

4. Especifique el nombre del paquete de instalación y haga clic en el botón **Examinar**.

   Se abre una ventana **Abrir** estándar para que elija el archivo de almacenamiento con el que se creará el paquete de instalación.

5. Seleccione un archivo de almacenamiento en alguna de las unidades 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 una aplicación de Kaspersky en el archivo de almacenamiento, verá un mensaje de error. Si necesita un paquete de instalación para una aplicación de Kaspersky, puede descargarlo de los servidores web de Kaspersky. Para acceder a esta operación, ingrese a **Operaciones → Aplicaciones de Kaspersky → Versiones actuales de las aplicaciones**.

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, introduzca los parámetros que desee agregar a la línea de comandos del archivo ejecutable.

   Puede agregar parámetros que permitan instalar la aplicación desde el paquete de instalación en modo silencioso. Para obtener detalles sobre los parámetros de línea de comandos, consulte la documentación del proveedor de la aplicación.

   Se inicia la creación del paquete de instalación.

   El asistente le informará cuando finalice el proceso.

   Si el paquete de instalación no se crea, verá un mensaje de error.

   En Kaspersky Security Center Cloud Console, el tamaño total combinado de los paquetes de instalación almacenados en el Servidor de administración no puede superar los 500 MB. Si se supera este límite de tamaño al crear el paquete de instalación, elimine los paquetes de instalación que haya creado antes. Encontrará el tamaño de cada paquete de instalación en sus propiedades.

8. Haga clic en el botón **Finalizar** para cerrar el asistente.

El nuevo paquete de instalación personalizado se descargará 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, encontrará las siguientes propiedades del 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.

Si desea cambiar el nombre o los parámetros de línea de comandos de un paquete de instalación personalizado, haga clic en el vínculo con el nombre de ese paquete en la lista de paquetes de instalación.

Requisitos para un punto de distribución

Para atender hasta 10000 dispositivos cliente, un punto de distribución debe reunir los siguientes requisitos mínimos (la configuración indicada es para un banco de prueba):

- CPU: Intel® Core™ i7-7700, 4 núcleos a 3,60 GHz.
- RAM: 8 GB.
- Espacio de almacenamiento libre: 120 GB.

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 **Descubrimiento y despliegue → Despliegue y asignación → Paquetes de instalación**.
   - En el menú principal, vaya a **Operaciones → Repositorios → Paquetes de instalación**.

   Se muestra una lista con los paquetes de instalación disponibles en el Servidor de administración.

2. Haga clic en el vínculo con el nombre del paquete de instalación del Agente de red.

   Se abre la ventana de propiedades del paquete de instalación del Agente de red. La información de la ventana está dividida en pestañas y en 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 forma predeterminada.

- **Instalar en la carpeta especificada**

  Si se selecciona esta opción, el Agente de red se instalará en la carpeta especificada en el campo de entrada.

El siguiente grupo de ajustes permite especificar una contraseña para la tarea de desinstalación remota del Agente de red:

- Utilizar contraseña de desinstalación

  Si habilita esta opción, podrá hacer clic en el botón **Modificar** para ingresar la contraseña de desinstalación (solo disponible para el Agente de red en dispositivos con sistemas operativos Windows).

  Esta opción está deshabilitada de forma predeterminada.

- **Estado**

- Evitar que el servicio del Agente de red se detenga o se elimine sin autorización e impedir cambios en su configuración

  Cuando esta opción está habilitada, una vez que el Agente de red se encuentre instalado en un dispositivo administrado, no se lo podrá eliminar ni reconfigurar a menos que se tengan los privilegios necesarios. El servicio del Agente de red no se podrá detener. Esta opción no tiene efecto en los controladores de dominio.

  Habilite esta opción para proteger el Agente de red en estaciones de trabajo operadas con derechos de administrador local.

  Esta opción está deshabilitada de forma predeterminada.

- Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes

  Si esta casilla está marcada, todas las actualizaciones y parches descargados para el Agente de red se instalarán automáticamente.

  Si esta casilla no está marcada, las actualizaciones y los parches que se descarguen se instalarán únicamente después de que su estado se cambie a *Aprobado*. Las actualizaciones y los parches con el estado *Sin definir* no se instalarán.

  Esta casilla está marcada de forma 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 los puertos del Agente de red en el Firewall de Microsoft Windows

  Cuando se habilita esta opción, se agregan los puertos que el Agente de red utiliza a la lista de exclusiones del Firewall de Microsoft Windows.

  Esta opción está activada de forma predeterminada.

- **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 forma 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 la 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:

- **Conectarse al Servidor de administración mediante una puerta de enlace de conexión**
- **Dirección de la puerta de enlace**
- Habilitar modo dinámico para VDI

  Si habilita esta opción, se habilitará un modo dinámico para infraestructuras de escritorios virtuales (VDI) para el Agente de red instalado en una máquina virtual.

  Esta opción está deshabilitada de forma predeterminada.

- Optimizar la configuración para VDI

Si habilita esta opción, se deshabilitarán las siguientes características de la configuración del Agente de red:

- Recopilación de información acerca del software instalado
- Recopilación de información acerca del hardware
- Recopilación de información acerca de las vulnerabilidades detectadas
- Recopilación de información acerca de las actualizaciones necesarias

Esta opción está deshabilitada de forma predeterminada.

- **Permitir la ejecución de la utilidad de registro de usuario luego de la instalación del Agente de red**

  Si esta opción está habilitada, la utilidad de registro del usuario como propietario del dispositivo se ejecutará después de la instalación del Agente de red. Esta opción está deshabilitada de forma predeterminada.

Componentes adicionales

En esta sección, puede seleccionar los componentes adicionales que desee instalar junto con el Agente de red.

Etiquetas

La sección **Etiquetas** muestra una lista de palabras claves (etiquetas) que se pueden agregar a los dispositivos cliente tras la instalación del Agente de red. Puede agregar etiquetas nuevas a la lista, así como eliminar las etiquetas existentes o cambiarles el nombre.

Si la casilla junto a una etiqueta está marcada, cuando se instale el Agente de red, la etiqueta correspondiente se agregará a los dispositivos administrados de manera automática.

Si la casilla junto a una etiqueta no está marcada, la etiqueta no se agregará automáticamente a los dispositivos administrados durante la instalación del Agente de red. De ser necesario, podrá agregar esa etiqueta manualmente a los dispositivos pertinentes.

Si elimina una etiqueta de la lista, se la eliminará automáticamente de todos los dispositivos a los que haya sido agregada.

Historial de revisiones

En esta sección, puede ver el historial de revisiones del paquete de instalación. Puede comparar las distintas revisiones, ver revisiones específicas, guardar revisiones en un archivo, agregar descripciones a las revisiones y modificar las descripciones existentes.

La siguiente tabla detalla los ajustes disponibles para el paquete de instalación del Agente de red según el sistema operativo.

Ajustes del paquete de instalación del Agente de red

Sección de propiedades	Windows	Mac	Linux
General	✓	✓	✓
Configuración	✓	—	—
Conexión	✓	✓	✓

		* excepto la casilla de verificación **Abrir los puertos del Agente de red en el Firewall de Microsoft Windows**	* excepto la casilla de verificación **Abrir los 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, le aconsejan que considere la deshabilitación de algunas funciones de Kaspersky Security Center Cloud Console que parecen ser de poco uso para máquinas virtuales.

Al instalar el Agente de red en una máquina virtual o en una plantilla querida para la generación de máquinas virtuales, recomendamos realizar las siguientes acciones:

- Si está ejecutando una instalación remota, en la ventana de propiedades del paquete de instalación del Agente de red, en la sección **Avanzado**, seleccione la opción **Optimizar la configuración para VDI**.
- Si está ejecutando una instalación interactiva a través de un Asistente, en la ventana Asistente, seleccione la opción **Optimizar la configuración del Agente de red para la infraestructura virtual**.

Seleccionar esas opciones cambia la configuración del Agente de red de modo que las funciones siguientes permanezcan desactivadas de forma predeterminada (antes de aplicar una directiva):

- Recopilación de información acerca del software instalado
- Recopilación de información acerca del hardware
- Recopilación de información acerca de las vulnerabilidades detectadas
- Recopilación de información acerca de las actualizaciones necesarias

Por lo general, esas funciones no son necesarias en máquinas virtuales porque usan el software uniforme y el hardware virtual.

La deshabilitación de las funciones es irreversible. Si alguna de las funciones desactivadas se requiere, la puede habilitar a través de la directiva del Agente de red, o a través de la configuración local del Agente de red. La configuración local del Agente de red está disponible a través del menú contextual del dispositivo relevante en la Consola de administración.

Compatibilidad con máquinas virtuales dinámicas

Kaspersky Security Center Cloud Console admite máquinas virtuales dinámicas. Si existe una infraestructura virtual en la red de la organización, las máquinas virtuales dinámicas (temporales) se pueden utilizar en ciertos casos. Las máquinas virtuales dinámicas se crean con nombres únicos según una plantilla que preparada por el administrador. El usuario trabaja en la máquina virtual un tiempo, luego, después de apagarse, esta máquina virtual se eliminará de la infraestructura virtual. La máquina virtual con el Agente de red instalado también se agrega a la base de datos del Servidor de administración. Después de desactivar 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 **Habilitar modo dinámico para VDI**:

- Para la instalación remota: En la ventana de propiedades del paquete de instalación del Agente de red (Sección **Avanzado**)
- Para la instalación interactiva: en el Asistente de instalación del Agente de red

Evite seleccionar la opción **Habilitar modo dinámico para VDI** al instalar el Agente de red en dispositivos físicos.

Si desea que los eventos de las máquinas virtuales dinámicas se almacenen en el Servidor de administración durante un tiempo después de eliminar esas máquinas virtuales, en la ventana de propiedades del Servidor de administración, en la sección **Repositorio de eventos**, marque la opción **Almacenar los eventos de los dispositivos eliminados** y especifique el plazo de almacenamiento máximo para los eventos (en días).

Soporte de copia de máquinas virtuales

Kaspersky Security Center Cloud Console es compatible con la copia de una máquina virtual con el Agente de red instalado o la creación de una máquina virtual desde una plantilla con el Agente de red instalado.

El Agente de red puede detectar de manera automática la copia de máquinas virtuales en los siguientes casos:

- La opción **Habilitar modo dinámico para VDI** se seleccionó cuando el Agente de red se instaló: después de cada reinicio del sistema operativo, esta máquina virtual se reconocerá como un dispositivo nuevo, sin tener en cuenta si se ha copiado.
- Uno de los siguientes hipervisores está en uso: VMware™, HyperV® o Xen®: Agente de red detecta la copia de la máquina virtual mediante los id. modificados del hardware virtual.

El análisis de cambios en el hardware virtual no es absolutamente fiable. Antes de aplicar este método extensamente, lo debe probar en un pequeño grupo de máquinas virtuales para la versión del hipervisor actualmente usado en su organización.

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. Los ajustes de la directiva y del paquete de instalación del Agente de red también difieren según el sistema operativo. La tabla de abajo compara las características del Agente de red y los escenarios de uso disponibles para los sistemas operativos Windows, macOS y Linux.

Comparación de funciones del Agente de red

Función del Agente de red	Windows	Linux	macOS
Instalación			
Instalación automática de actualizaciones y 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 infraestructura de escritorio virtual (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 aparecen en las propiedades del punto de distribución, pero las funciones correspondientes no están disponibles en el Agente de red para macOS:

- 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** → **Ajustes específicos de Unix**.

4. Configure los siguientes ajustes:

   - **Definir una contraseña para la cuenta root (solo para despliegues a través de SSH)**

     Si el comando `sudo` no se puede utilizar en el dispositivo de destino sin introducir la contraseña, seleccione esta opción y especifique la contraseña de la cuenta root. Kaspersky Security Center Cloud Console transmitirá la contraseña de forma cifrada al dispositivo de destino, la descifrará y, finalmente, la utilizará para iniciar el procedimiento de instalación en nombre de la cuenta root.

     Kaspersky Security Center Cloud Console no usará la cuenta ni la contraseña especificada para crear una conexión SSH.

   - **Especificar la ruta a una carpeta temporal con permisos de ejecución en el dispositivo de destino (solo para despliegues a través de SSH)**

     Si el directorio /tmp del dispositivo de destino no tiene permiso de ejecución, seleccione esta opción y, a continuación, especifique la ruta a un directorio que sí tenga permiso de ejecución. Kaspersky Security Center 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

Para instalar una aplicación de seguridad de Kaspersky a través de Kaspersky Security Center Cloud Console, es posible que deba desinstalar aplicaciones desarrolladas por un tercero que no sean compatibles con la aplicación que quiera instalar. Kaspersky Security Center Cloud Console ofrece varias formas de eliminar 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 aplicaciones incompatibles automáticamente**. La opción es parte del Asistente de despliegue de la protección. Cuando esta opción está habilitada, Kaspersky Security Center Cloud Console elimina las aplicaciones incompatibles antes de instalar una aplicación de seguridad en un dispositivo administrado.

Eliminar aplicaciones incompatibles a través de una tarea dedicada

Para eliminar aplicaciones incompatibles a través de una tarea, use la tarea **Desinstalar aplicación de forma remota**. Esta tarea se debe ejecutar en los dispositivos antes que la tarea para instalar la aplicación de seguridad. Por ejemplo, en la tarea de instalación, puede seleccionar **Al completar otra tarea** como tipo de programación, donde la otra tarea es **Desinstalar aplicación de forma remota**.

Este método de desinstalación es útil cuando el instalador de la aplicación de seguridad no puede eliminar correctamente una aplicación incompatible.

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 desplegar por primera vez el Agente de red u otras aplicaciones, puede forzar la instalación de los paquetes de instalación seleccionados con la tarea de instalación remota de Kaspersky Security Center Cloud Console, siempre que cada dispositivo tenga una cuenta de usuario con derechos de administrador local.

En el primer despliegue, el Agente de red no está instalado. Por lo tanto, en la configuración de la tarea de instalación remota, no se puede seleccionar la distribución de los archivos necesarios para la instalación de la aplicación mediante el Agente de red. Solo puede optar por distribuir archivos con recursos del sistema operativo a través 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), mediante la selección del grupo de administración de Kaspersky Security Center Cloud Console al cual pertenecen o tras crear una selección de dispositivos en función de un criterio específico. La hora de inicio de instalación es definida por la programación de la tarea. Si la configuración **Ejecutar tareas no realizadas** se habilita en las propiedades de la tarea, la tarea se puede ejecutar inmediatamente después de que los dispositivos de destino se activen, o cuando se muevan al grupo de administración de destino.

La instalación forzada consiste en el envío de paquetes de instalación a dispositivos de destino, la copia subsecuente de archivos al recurso admin$ en cada uno de los dispositivos de destino y el registro remoto de los servicios de compatibilidad en esos dispositivos. La entrega de paquetes de instalación a dispositivos de destino se realiza mediante una función de Kaspersky Security Center 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 están en ejecución en los dispositivos de destino:
  - Servidor (LanmanServer)

De manera predeterminada, este servicio está en ejecución.

- Iniciador de procesos de servidor DCOM (DcomLaunch)
- Asignador de endpoints RPC (RpcEptMapper)
- Llamada a procedimiento remoto (RpcSs)

- El puerto TCP 445 está abierto en los dispositivos de destino para permitir el acceso remoto a través del Instrumental de administración de Windows.

  TCP 139, UDP 137 y UDP 138 se usan en protocolos más antiguos y ya no son necesarios para las aplicaciones actuales.

  En el firewall, se deben permitir puertos de acceso saliente dinámicos para las conexiones desde los puntos de distribución a los dispositivos de destino.

- Se permiten configuraciones de seguridad de la política de dominio de Active Directory para el funcionamiento del protocolo NTLM durante el despliegue del Agente de red.
- En los dispositivos de destino que ejecutan Microsoft Windows XP, el modo de uso compartido simple de archivos está deshabilitado.
- En los dispositivos de destino, el modelo de seguridad y uso compartido de acceso se configura como *Clásico: los usuarios locales se autentican como ellos mismos*. De ninguna manera puede ser *Invitado únicamente: los usuarios locales se autentican como invitados*.
- Los dispositivos de destino son miembros del dominio, o bien se crean cuentas uniformes con derechos de administrador en los dispositivos de destino de antemano.

Para desplegar correctamente el Agente de red u otras aplicaciones en un dispositivo que no está unido a un dominio de Active Directory de Windows Server 2003 o posterior, debe deshabilitar el Control de cuentas de usuario (UAC) remoto en el dispositivo. UAC remoto es una de las razones que impide que las cuentas de administradores locales accedan a admin$, lo que es necesario para el despliegue forzado del Agente de red u otras aplicaciones. Si deshabilita UAC remoto, no interfiere con UAC local.

Durante la instalación en dispositivos nuevos que todavía no se asignaron 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 forma simplificada de crear tareas para la instalación forzada de aplicaciones es la instalación automática. Para hacerlo, abra las propiedades del grupo de administración, abra la lista de paquetes de instalación y seleccione los que se deben instalar en dispositivos de este grupo. Como resultado, los paquetes de instalación seleccionados se instalarán automáticamente en todos los dispositivos de este grupo y todos sus subgrupos. El intervalo de tiempo durante el cual los paquetes se instalarán depende del rendimiento de la red y el número total de dispositivos conectados a una red.

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 **Descubrimiento y despliegue → Despliegue y asignación → Paquetes de instalación**. El paquete puede usarse para instalar la aplicación en otro momento.
- Crea y ejecuta una tarea de instalación remota para dispositivos específicos o para un grupo de administración. La nueva tarea de instalación remota se agrega a la sección **Tareas**. Podrá iniciar la tarea manualmente cuando lo desee. El tipo de tarea es **Instalar aplicación de forma remota**.

Paso 1. Iniciar el Asistente de despliegue de la protección

Para iniciar manualmente el Asistente de despliegue de la protección,

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

Se abre el Asistente de despliegue de la protección. Avance por el asistente utilizando el botón **Siguiente**.

Paso 1. Seleccionar el paquete de instalación

Seleccione la forma en que desea instalar el paquete de instalación seleccionado:

- **Instalación remota mediante Kaspersky Security Center**
- **Instalación remota mediante Microsoft Azure API**

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 **Agregar** 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 los dispositivos para la instalación**

  La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

  Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

Paso 4. Configurar la tarea de instalación remota

En la página de **configuración de la tarea "Instalación remota"**, especifique la configuración para la instalación remota de la aplicación.

En el grupo de configuraciones **Forzar la descarga del paquete de instalación**, especifique cómo los archivos necesarios para la instalación de la aplicación se distribuyen a los dispositivos cliente:

- **Con el Agente de red**

  Si habilita esta opción, los paquetes de instalación se transferirán a los dispositivos cliente a través del Agente de red instalado en esos dispositivos.

  Si no habilita esta opción, los paquetes de instalación se distribuirán utilizando las herramientas provistas por el sistema operativo de los dispositivos cliente.

  Recomendamos habilitar esta opción si la tarea está asignada a dispositivos que tienen instalado el Agente de red.

  Esta opción está habilitada de manera predeterminada.

- **Con los recursos del sistema operativo a través de los puntos de distribución**

Si habilita esta opción, los paquetes de instalación se transferirán a los dispositivos cliente mediante las herramientas del sistema operativo a través de los puntos de distribución. Puede seleccionar esta opción si existe al menos un punto de distribución en la red.

Si habilitó la opción **Con el Agente de red**, las herramientas del sistema operativo se utilizarán para transferir los archivos solo si las herramientas del Agente de red no están disponibles.

Está opción se habilita de manera predeterminada para las tareas de instalación remota creadas en servidores de administración virtuales.

Defina la configuración adicional:

No reinstalar la aplicación si ya está instalada

Si habilita esta opción y se detecta que la aplicación ya está instalada en el dispositivo cliente, no se la reinstalará.

Si no habilita esta opción, la aplicación se instalará en todos los casos.

Esta opción está activada de forma predeterminada.

Contraseña para desinstalar la aplicación de Kaspersky actual

El campo **Contraseña para desinstalar la aplicación de Kaspersky actual** solo está disponible si seleccionó la opción **Con el Agente de red** en el grupo de configuración **Forzar la descarga del paquete de instalación**.

Ingrese 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 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 mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

    Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

    Si no habilita esta opción, la solicitud se mostrará una sola vez.

  - **Reiniciar después de (min)**

    Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

    Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

  Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

  Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

  Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

  Esta opción está deshabilitada de forma predeterminada.

Paso 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 la opción si desea que Kaspersky Security Center Cloud Console elimine automáticamente las aplicaciones que sean incompatibles con la aplicación que se va a desplegar.

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 los dispositivos**

  Los dispositivos se mantendrán en los grupos en los que se encuentren. Los dispositivos que no pertenezcan a ningún grupo quedarán sin asignar.

- **Mover los dispositivos no asignados a un grupo**

  Los dispositivos se moverán al grupo de administración que seleccione.

La opción **No mover los dispositivos** está seleccionada de manera predeterminada. Es posible que quiera mover los dispositivos manualmente por seguridad.

Paso 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 se necesita una cuenta (el Agente de red está instalado)**

  Si selecciona esta opción, no necesitará especificar la cuenta con la que se ejecutará el instalador de la aplicación. Para ejecutar la tarea, se usará la cuenta con la que se haya iniciado el servicio del Servidor de administración.

  Esta opción no está disponible si el Agente de red no se instaló en los dispositivos cliente.

- **Se necesita una cuenta (no se utiliza el Agente de red)**

Seleccione esta opción si el Agente de red no está instalado en los dispositivos a los que asigna la tarea de instalación remota. En este caso, puede especificar una cuenta de usuario o un certificado SSH para instalar la aplicación.

- **Cuenta local**. Si se selecciona esta opción, especifique la cuenta bajo la que se ejecutará el instalador de aplicación. Haga clic en el botón **Agregar**, seleccione **Cuenta local** y, a continuación, especifique las credenciales de la cuenta de usuario.

  Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que asigne esta tarea. En este caso, todas las cuentas añadidas se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

- **Certificado de SSH**. Si desea instalar una aplicación en un dispositivo cliente basado en Linux, puede especificar un certificado SSH en lugar de una cuenta de usuario. Haga clic en el botón **Agregar**, seleccione **Certificado de SSH** y, a continuación, especifique las claves pública y privada del certificado.

  Para generar una clave privada, puede utilizar la utilidad ssh-keygen. Tenga en cuenta que Kaspersky Security Center 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. Inicio de la instalación

Esta página es el último paso del asistente. En este paso, la tarea **Tarea de instalación remota** está correctamente creada y configurada.

De manera predeterminada, la opción **Ejecutar la tarea al finalizar el asistente** no está seleccionada. Si selecciona esta opción, la tarea **Tarea de instalación remota** comenzará inmediatamente después de que complete el asistente. Si no selecciona esta opción, la tarea **Tarea de instalación remota** no comenzará. Podrá iniciar la tarea manualmente cuando lo desee.

Haga clic en **Aceptar** para completar el paso final del Asistente de despliegue de la protección.

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

	https://s03.upd.kaspersky.com 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 verifica que haya acceso a los servidores de Kaspersky. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos.
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	Actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky.

	http://downloads8.kaspersky-labs.com 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	Novedades con fines publicitarios.

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 desee instalar el Agente de red para 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 estas instrucciones utilizando una cuenta con privilegios de root.

Para preparar un dispositivo que ejecuta Astra Linux en el modo de entorno de software cerrado para la instalación del Agente de red:

1. Abra el archivo `/etc/digsig/digsig_initramfs.conf` y 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 vínculo: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Actualice los discos RAM:

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

   Reinicie el sistema.

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 abrí'o, 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 agregue la última línea con el siguiente texto: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

d. Guarde el archivo sudoers y, luego, ciérrelo.

e. Conéctese al dispositivo de nuevo mediante SSH y asegúrese de que servicio de sudo no le solicite una contraseña. Puede hacerlo mediante el comando `sudo whoami`.

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, agregue la cadena `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` en el archivo `/home/<username>/.bashrc`, en el que < `username` > 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, seleccione la casilla **Uso de los recursos del sistema operativo a través del Servidor de administración**. Quite la selección a todo.
   - En la página **Seleccione una cuenta para ejecutar la tarea**, especifique la configuración de la cuenta de usuario que se utiliza para la conexión del dispositivo mediante SSH.
3. Ejecute la tarea de instalación remota. Utilice la opción para el comando `su` para preservar el 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 los dispositivos a través de un asistente específico. Para asignar una tarea con mayor facilidad y rapidez, puede especificar los dispositivos (hasta 1000) de distintas maneras a través de la ventana del asistente:

- **Seleccionar dispositivos de la red detectados por el Servidor de administración**. En este caso, la tarea se asigna a dispositivos específicos. Estos pueden ser tanto dispositivos asignados a grupos de administración como dispositivos no asignados.
- **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**. En este caso, puede especificar nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.
- **Asignar tarea a una selección de dispositivos**. En este caso, la tarea se asigna a los dispositivos incluidos en una selección creada anteriormente. Puede especificar la selección predeterminada o una personalizada que 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

En este artículo, se explica cómo instalar una aplicación de forma remota en los 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 **Agregar**.

   Se inicia el Asistente para crear nueva tarea.

3. En la sección **Tipo de tarea**, seleccione **Instalar aplicación de forma remota**.

4. Seleccione una de las siguientes opciones:

   - **Asignar tarea a un grupo de administración**

     La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

     Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

     Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

   - **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**

     Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

     Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

   - **Asignar tarea a una selección de dispositivos**

     La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

     Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

   La tarea *Instalar aplicación de forma remota* se creará para los dispositivos especificados. Si seleccionó la opción **Asignar tarea a un grupo de administración**, la tarea será una tarea de grupo.

5. En el paso **Alcance de la tarea**, indique un grupo de administración, dispositivos con direcciones específicas o una selección de dispositivos.

   Los ajustes disponibles dependerán de la opción seleccionada en el paso anterior.

6. En el paso **Paquetes de instalación**, defina los siguientes ajustes:

   - Seleccione cómo desea instalar la aplicación seleccionada:

     - **Instalación remota mediante Kaspersky Security Center**

     - **Instalación remota mediante Microsoft Azure API**

       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 **Seleccionar paquete de instalación**, seleccione el paquete de instalación de la aplicación que desee instalar.

- En el grupo de configuraciones **Forzar la descarga del paquete de instalación**, puede especificar cómo se distribuyen a los dispositivos cliente los archivos que se requieren para la instalación de una aplicación:

  - **Con el Agente de red**

    Si habilita esta opción, los paquetes de instalación se transferirán a los dispositivos cliente a través del Agente de red instalado en esos dispositivos.

    Si no habilita esta opción, los paquetes de instalación se distribuirán utilizando las herramientas provistas por el sistema operativo de los dispositivos cliente.

    Recomendamos habilitar esta opción si la tarea está asignada a dispositivos que tienen instalado el Agente de red.

    Esta opción está habilitada de manera predeterminada.

  - **Con los recursos del sistema operativo a través de los puntos de distribución**

    Si habilita esta opción, los paquetes de instalación se transferirán a los dispositivos cliente mediante las herramientas del sistema operativo a través de los puntos de distribución. Puede seleccionar esta opción si existe al menos un punto de distribución en la red.

    Si habilitó la opción **Con el Agente de red**, las herramientas del sistema operativo se utilizarán para transferir los archivos solo si las herramientas del Agente de red no están disponibles.

    Está opción se habilita de manera predeterminada para las tareas de instalación remota creadas en servidores de administración virtuales.

- En el campo **Número máximo de descargas simultáneas**, ingrese el número máximo permitido de dispositivos cliente a los que el Servidor de administración podrá transmitir simultáneamente los archivos.

- En el campo **Número máximo de intentos de instalación**, ingrese el límite de veces que se podrá ejecutar el instalador.

  Si se supera la cantidad de intentos indicados con este parámetro, Kaspersky Security Center Cloud Console dejará de iniciar el instalador en el dispositivo. Para reiniciar la tarea *Instalar aplicación de forma remota*, aumente el valor del parámetro **Número máximo de intentos de instalación** y reinicie la tarea. Como alternativa, cree una nueva tarea *Instalar aplicación de forma remota*.

- Si migra de una aplicación de Kaspersky a otra y su aplicación actual está protegida con contraseña, ingrese la contraseña en el campo **Contraseña para desinstalar la aplicación de Kaspersky actual**. Tenga en cuenta que durante la migración, se desinstalará su aplicación de Kaspersky actual.

  El campo **Contraseña para desinstalar la aplicación de Kaspersky actual** solo está disponible si seleccionó la opción **Con el Agente de red** en el grupo de configuración **Forzar la descarga del paquete de instalación**.

  Puede usar la contraseña de desinstalación solo para la migración de Kaspersky Security para Windows Server a Kaspersky Endpoint Security para Windows al instalar Kaspersky Endpoint Security para Windows mediante la tarea *Instalar aplicación de forma remota*. El uso de la contraseña de desinstalación al instalar otras aplicaciones puede causar errores de instalación.

  Para completar el escenario de migración correctamente, asegúrese de que se cumplan los siguientes requisitos previos:

  - Está utilizando el Agente de red de Kaspersky Security Center 14.2 para Windows o una versión posterior.

- Está instalando la aplicación en dispositivos con Windows.

- Defina las opciones adicionales:

  - **No reinstalar la aplicación si ya está instalada**

    Si habilita esta opción y se detecta que la aplicación ya está instalada en el dispositivo cliente, no se la reinstalará.

    Si no habilita esta opción, la aplicación se instalará en todos los casos.

    Esta opción está activada de forma predeterminada.

  - **Verificar el tipo de sistema operativo antes de la descarga**

    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 ni 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.

  - **Solicitar a los usuarios que cierren las aplicaciones en ejecución**

    Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

    Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

    Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

    Esta opción está deshabilitada de forma predeterminada.

- Seleccione los dispositivos en los que desee instalar la aplicación:

  - **Instalar en todos los dispositivos**

    La aplicación se instalará incluso en dispositivos administrados por otros Servidores de administración.

    Esta opción está seleccionada de manera predeterminada. Si solo tiene un Servidor de administración en la red, no es necesario que cambie esta opción.

  - **Instalar solo en dispositivos administrados a través de este Servidor de administración**

    La aplicación se instalará solo en los dispositivos administrados por este Servidor de administración. Seleccione esta opción si tiene más de un Servidor de administración en su red y desea evitar conflictos entre ellos.

- Indique si los dispositivos deberán moverse a un grupo de administración después de la instalación:
  - **No mover los dispositivos**

    Los dispositivos se mantendrán en los grupos en los que se encuentren. Los dispositivos que no pertenezcan a ningún grupo quedarán sin asignar.

  - **Mover los dispositivos no asignados a este grupo (no se puede seleccionar más de un grupo)**

    Los dispositivos se moverán al grupo de administración que seleccione.

  La opción **No mover los dispositivos** está seleccionada de manera predeterminada. Es posible que quiera mover los dispositivos manualmente por seguridad.

7. En este paso del asistente, indique si los dispositivos deberán reiniciarse durante la instalación de las aplicaciones:
   - **No reiniciar el dispositivo**

     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 forma predeterminada.

     - **Repetir solicitud cada (min)**

       Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

       Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

       Si no habilita esta opción, la solicitud se mostrará una sola vez.

     - **Reiniciar después de (min)**

Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

  Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

  Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

  Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

  Esta opción está deshabilitada de forma predeterminada.

8. De ser necesario, en el paso **Seleccione las cuentas con las que se accederá a los dispositivos**, agregue las cuentas que se utilizarán para iniciar la tarea *Instalar aplicación de forma remota*:

   - **No se necesita una cuenta (el Agente de red está instalado)**

     Si selecciona esta opción, no necesitará especificar la cuenta con la que se ejecutará el instalador de la aplicación. Para ejecutar la tarea, se usará la cuenta con la que se haya iniciado el servicio del Servidor de administración.

     Esta opción no está disponible si el Agente de red no se instaló en los dispositivos cliente.

   - **Se necesita una cuenta (no se utiliza el Agente de red)**

Seleccione esta opción si el Agente de red no está instalado en los dispositivos a los que asigna la tarea de instalación remota. En este caso, puede especificar una cuenta de usuario o un certificado SSH para instalar la aplicación.

- **Cuenta local**. Si se selecciona esta opción, especifique la cuenta bajo la que se ejecutará el instalador de aplicación. Haga clic en el botón **Agregar**, seleccione **Cuenta local** y, a continuación, especifique las credenciales de la cuenta de usuario.

  Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que asigne esta tarea. En este caso, todas las cuentas añadidas se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

- **Certificado de SSH**. Si desea instalar una aplicación en un dispositivo cliente basado en Linux, puede especificar un certificado SSH en lugar de una cuenta de usuario. Haga clic en el botón **Agregar**, seleccione **Certificado de SSH** y, a continuación, especifique las claves pública y privada del certificado.

  Para generar una clave privada, puede utilizar la utilidad ssh-keygen. Tenga en cuenta que Kaspersky Security Center 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 la tarea**, haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

   Si habilitó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abrirá la ventana de configuración de la tarea. Utilice esta ventana para, de ser necesario, revisar y modificar los ajustes de la tarea o programar su ejecución.

10. En la lista de tareas, seleccione la tarea creada y haga clic en **Iniciar**.

    Como alternativa, puede esperar a que ocurra el inicio programado definido en los ajustes de la tarea.

Cuando se completa la tarea de instalación remota, la aplicación seleccionada se instala en los dispositivos especificados.

Instalar aplicaciones en los Servidores de administración secundarios

Para instalar una aplicación en Servidores de administración secundarios:

1. Establezca conexión con el Servidor de administración que controla los servidores de administración secundarios pertinentes.

2. Asegúrese de que el paquete de instalación que corresponde a la aplicación que se está instalando esté disponible en cada uno de los Servidores de administración secundarios seleccionados. Si no puede encontrar el paquete de instalación en ninguno de los servidores secundarios, distribúyalo. Para este propósito, cree una tarea con el tipo de tarea **Distribuir paquete de instalación**.

3. Crear una tarea para la instalación de una aplicación remota en Servidores de administración secundarios. Seleccione el tipo de actividad de **Instalar aplicación en el Servidor de administración secundario de forma remota**.

El Asistente para crear nueva tarea creará la tarea para instalar de manera remota, en servidores de administración secundarios específicos, la aplicación seleccionada en el asistente.

4. Ejecute la tarea manualmente o espere a que se inicie según la programación configurada para la tarea.

Cuando se completa la tarea de instalación remota, la aplicación seleccionada se instala en los Servidores de administración secundarios.

Iniciar y detener aplicaciones de Kaspersky

Puede usar la tarea *Iniciar o detener aplicación* para iniciar y detener aplicaciones de Kaspersky en los dispositivos administrados.

Para crear la tarea Iniciar o detener aplicación:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
3. En la lista desplegable **Aplicación**, seleccione la aplicación para la que desea crear la tarea.
4. En la lista **Tipo de tarea**, seleccione la tarea **Activación de la aplicación**.
5. En el campo **Nombre de la tarea**, ingrese el nombre de la tarea nueva.

   El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
6. Seleccione los dispositivos a los que se asignará la tarea.
7. En la ventana **Aplicaciones**, haga lo siguiente:
   - Marque las casillas junto a los nombres de las aplicaciones para las que desee crear la tarea.
   - Seleccione la opción **Iniciar la aplicación** o **Detener la aplicación**.
8. Si desea modificar la configuración predeterminada de la tarea, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en el paso **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.
9. Haga clic en el botón **Finalizar**.

   Se crea la tarea y se la agrega a la lista de tareas.
10. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.
11. En la ventana de propiedades de la tarea, defina los ajustes generales de la tarea que se adapten a sus necesidades y luego guárdelos.

La tarea queda creada y configurada.

Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

Administración de dispositivos móviles

La administración de 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 de los dispositivos depende de la aplicación Kaspersky Security para dispositivos móviles. Esta app mantendrá los dispositivos a resguardo de virus, amenazas web y otros programas que puedan resultar peligrosos.

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.

Funciones de detección y respuesta

En esta sección, encontrará información sobre las soluciones de Kaspersky que puede integrar en Kaspersky Security Center Cloud Console para agregar funciones de detección y respuesta a la consola.

Acerca de las funciones de detección y respuesta

Kaspersky Security Center Cloud Console puede integrar funciones de otras soluciones de Kaspersky en la interfaz de la consola. Ello permite, por ejemplo, agregar funciones de detección y respuesta a las características de Kaspersky Security Center Cloud Console.

Las soluciones de detección y respuesta están diseñadas para proteger la infraestructura de TI de una organización de ciberamenazas complejas. Combinan tecnologías de autodetección de amenazas con la capacidad de responder a los riesgos encontrados para resistir ataques complejos, como los ataques sin archivo, el abuso de herramientas estándar del sistema y los ataques que permiten montar el ransomware y los nuevos exploits.

Las soluciones que se pueden integrar son las siguientes:

- Kaspersky Endpoint Detection and Response Optimum

  Cuando una aplicación EPP (siglas en inglés de "plataforma de protección de endpoints") de Kaspersky detecta una amenaza, Kaspersky Security Center Cloud Console agrega una alerta a la lista de alertas. La alerta contiene los detalles de la amenaza detectada y permite analizarla e investigarla. La amenaza también se puede examinar en forma visual, a través de un gráfico que representa la cadena de desarrollo de la amenaza. El gráfico describe las etapas de despliegue del ataque detectado a lo largo del tiempo.

  Para responder a un incidente, puede elegirse una de las acciones predefinidas: aislar el objeto no confiable, crear una regla que impida su ejecución, aislar el dispositivo vulnerado de la red y otras.

  Para ver detalles sobre cómo activar esta solución, consulte la documentación de Kaspersky Endpoint Detection and Response Optimum.

- Kaspersky Managed Detection and Response

  Cuando una aplicación EPP de Kaspersky detecta una amenaza, Kaspersky Security Center Cloud Console agrega un incidente a la lista de incidentes. Los incidentes contienen información detallada sobre la amenaza detectada. Los analistas de los centros de operaciones de seguridad (SOC) de MDR de Kaspersky o de una empresa externa investigan los incidentes y ofrecen respuestas para resolverlos. Usted puede aceptar o rechazar manualmente las medidas que se le ofrecen o puede activar una opción para que las respuestas siempre se acepten automáticamente.

  Para ver detalles sobre cómo activar esta solución, consulte la documentación de Kaspersky Managed Detection and Response.

- Kaspersky Endpoint Detection and Response Expert

  Se trata de una solución para organizaciones que cuentan con un equipo de analistas de SOC. Las amenazas detectadas se registran como alertas o incidentes que pueden asignarse a analistas de SOC para que se ocupen de su investigación. Kaspersky Endpoint Detection and Response Expert le ofrece información detallada acerca de cada alerta o incidente, así como también las herramientas para la administración de alertas o incidentes, búsqueda de amenazas y desarrollo de reglas personalizadas. Los analistas o directores de seguridad de SOC pueden seleccionar las acciones de respuesta de manera manual o bien se pueden tomar las medidas de respuesta automatizada predefinidas.

  Para obtener información acerca de la activación de la solución, consulte la documentación sobre Kaspersky Endpoint Detection and Response Expert.

Cambios en la interfaz tras integrar las funciones de detección y respuesta

Las siguientes soluciones de Kaspersky ofrecen 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

En la siguiente tabla, se enumeran los cambios que estas soluciones realizan en la interfaz de Kaspersky Security Center Cloud Console luego de la integración.

Cambios realizados en la interfaz por las soluciones de Kaspersky integradas

Solución	Cambios en Kaspersky Security Center Cloud Console
Kaspersky EDR Optimum	Se agregan los siguientes elementos: • La sección **Alertas** (**Supervisión e informes** → **Alertas**). Las alertas detectadas por esta solución se enumeran en la pestaña **Optimum**. • Un widget en el **Panel** (**Supervisión e informes** → **Panel**).
Kaspersky MDR	Se agregan los siguientes elementos: • La sección **MDR** (**Supervisión e informes** → **MDR**). • La opción **Mostrar funciones de MDR** (**Configuración** → **Opciones de interfaz** → **Mostrar funciones de MDR**). • Un widget en el **Panel** (**Supervisión e informes** → **Panel**).
Kaspersky EDR Expert	Se agregan los siguientes elementos: • La sección **Alertas** (**Supervisión e informes** → **Alertas**). Las alertas detectadas por esta solución se enumeran en la pestaña **Experto**. • Sección **Incidentes** (**Supervisión e informes** → **Incidentes**). • Sección **Búsqueda de amenazas** (**Supervisión e informes** → **Búsqueda de amenazas**). • Sección **Reglas personalizadas** (**Supervisión e informes** → **Reglas personalizadas**). • Configuración general de Kaspersky EDR Expert (**Configuración**→ **Integración** → **Kaspersky EDR Expert**). • Widgets en **Panel** (**Supervisión e informes** → **Panel**).

Descubrir dispositivos en red y crear grupos de administración

En esta sección, se describen la función de búsqueda y descubrimiento de dispositivos conectados a la red y el proceso para crear grupos de administración para esos dispositivos.

Kaspersky Security Center Cloud Console permite buscar dispositivos utilizando criterios específicos. Los resultados de estas búsquedas se pueden guardar en un archivo de texto.

La función de búsqueda y descubrimiento permite hallar los siguientes dispositivos:

- Dispositivos administrados que pertenecen a los grupos de administración tanto del Servidor de administración de Kaspersky Security Center Cloud Console como de sus servidores de administración secundarios.
- Dispositivos no asignados que son administrados por el Servidor de administración de Kaspersky Security Center Cloud Console o por alguno de sus servidores de administración secundarios.

Escenario: Descubrir dispositivos conectados a la red

Antes de realizar el despliegue inicial de las aplicaciones de seguridad, se debe llevar a cabo un proceso denominado "descubrimiento de dispositivos". Descubrir qué dispositivos están conectados a la red permite recibir información sobre ellos y administrarlos mediante directivas. La red debe sondearse en forma periódica para hallar dispositivos nuevos y determinar si los que ya se habían descubierto siguen conectados.

Al concluir este escenario, el proceso de descubrimiento se llevará a cabo siguiendo la programación y la configuración que especifique.

Requisitos previos

En Kaspersky Security Center Cloud Console, el descubrimiento de dispositivos es una tarea realizada por los puntos de distribución. Antes de comenzar, haga lo siguiente:

- Decida qué dispositivos actuarán como puntos de distribución.
- Instale el Agente de red en los dispositivos elegidos.
- Designe esos dispositivos como puntos de distribución manualmente.

Etapas

El escenario se divide en etapas:

1. **Elegir los tipos de descubrimiento**

   Decida qué tipos de detección desea utilizar regularmente.

2. **Configurar los sondeos**

   En las propiedades de cada punto de distribución, habilite y configure los tipos de sondeo de red que haya elegido: sondeo de la red de Windows, sondeo del controlador de dominio o sondeo de intervalos IP. Verifique que la programación de los sondeos se ajuste a las necesidades de su organización.

   Si se incluyen dispositivos en red en un dominio, se recomienda utilizar el sondeo de controlador de dominio.

3. **Configurar reglas para que los dispositivos descubiertos se agreguen a grupos de administración (opcional)**

   Si aparecen nuevos dispositivos en la red, se detectarán durante las encuestas regulares y se incluirán 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 no configura ninguna regla, los dispositivos descubiertos se agregarán al grupo **Dispositivos no asignados** y se dejarán allí. Si lo desea, podrá mover esos dispositivos al grupo **Dispositivos administrados** manualmente. Si mueve los dispositivos manualmente al grupo **Dispositivos administrados**, puede analizar la información sobre cada dispositivo y decidir si desea moverlo a un grupo de administración, y, de ser así, a qué grupo exacto.

Cuando se complete una operación de sondeo, verifique que los nuevos dispositivos se hayan organizado según las reglas configuradas. Si no configura ninguna regla, los dispositivos se dejarán en el grupo **Dispositivos no asignados**.

Sondeo de red

La información sobre la estructura de la red y los dispositivos de esta red la recibe Kaspersky Security Center Cloud Console a través de sondeos regulares de la red de Windows, intervalos IP, un controlador de dominio de Microsoft Active Directory y un controlador de dominio de Samba. Para un controlador de dominio de Samba, Samba 4 se utiliza como controlador de dominio de Active Directory. El proceso de sondeo puede iniciarse de forma automática (siguiendo una programación) o de forma manual.

Kaspersky Security Center Cloud Console utiliza el resultado de los sondeos para actualizar la lista de dispositivos no asignados. Si lo desea, puede configurar reglas que harán que los dispositivos descubiertos en cada sondeo se muevan a distintos grupos de administración automáticamente.

Kaspersky Security Center Cloud Console utiliza los siguientes métodos de sondeo de red:

- *Sondeo de intervalos IP*. Kaspersky Security Center Cloud Console utiliza paquetes ICMP (el protocolo de mensajes de control de Internet) para sondear los intervalos IP que se le indican y recopilar un conjunto de datos completo sobre los dispositivos con direcciones IP de esos intervalos.

- *Sondeo de la red de Windows*. Existen dos modos para sondear la red de Windows: rápido y completo. Cuando se realiza un sondeo rápido, Kaspersky Security Center Cloud Console 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 le solicita la siguiente información a cada dispositivo: sistema operativo (SO), dirección IP, nombre DNS y nombre NetBIOS.

- *Sondeo de controladores de dominio*. Cuando se realiza este tipo de sondeo, se recupera información sobre la estructura de las unidades de Active Directory y sobre los nombres DNS de los dispositivos incluidos en los grupos de Active Directory. La información recabada se registra en la base de datos de Kaspersky Security Center Cloud Console.

Los resultados del sondeo se muestran en la sección **Descubrimiento y despliegue → Descubrimiento** por separado para los métodos de *Sondeo de la red de Windows* y *Sondeo de controladores de dominio*.

Los resultados del sondeo para el método de *Sondeo de intervalos IP* se muestran en la sección **Descubrimiento y despliegue → Dispositivos no asignados**.

Un mismo dispositivo puede aparecer 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 las opciones de sondeo de cada método. 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:

- Los puertos UDP 137/138 y TCP 139 deben estar disponibles 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 desee 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 **Habilitar sondeo de red**, habilite o deshabilite el sondeo de la red de Windows.
6. Configure la programación del sondeo rápido y del 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 de 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 con la programación que usted define.

Requisitos previos

Antes de sondear un controlador de dominio, asegúrese de que los siguientes protocolos están habilitados:

- 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 de controlador de dominio:

- 389 para SASL
- 636 para TLS

Sondeo de controlador de dominio mediante el uso de 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 de Microsoft Active Directory.
No se admite el sondeo con un punto de distribución de Mac.

Para configurar el sondeo de controlador de dominio mediante el punto de distribución:

1. Abra las propiedades del punto de distribución.
2. Seleccione la sección **Sondeo del controlador de dominio**.

3. Seleccione la opción **Habilitar el sondeo de controladores de dominio**.

4. Seleccione el controlador de dominio que desea sondear.

   Si utiliza un punto de distribución de Linux, en la sección **Sondear dominios específicos**, haga clic en **Agregar** y luego especifique la dirección y las credenciales de usuario del controlador de dominio.

   Si utiliza un punto de distribución de Windows, puede seleccionar una de las siguientes opciones:

   - **Sondear dominio actual**
   - **Sondear bosque de dominio entero**
   - **Sondear dominios específicos**

5. Haga clic en el botón **Establecer programación de sondeo** para especificar las opciones del programa de sondeo si es necesario.

   El sondeo comenzará según el programa especificado únicamente. El inicio manual del sondeo no está disponible.

Una vez completado el sondeo, la estructura del dominio se mostrará en la sección **Controladores de dominio**.

Si configura y habilita reglas de movimiento de dispositivos, los dispositivos recién detectados 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:

1. En el menú principal, vaya a **Descubrimiento y despliegue** → **Descubrimiento** → **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 lleva a cabo una operación de resolución inversa para intentar determinar, mediante consultas DNS estándar, el nombre DNS correspondiente a cada dirección del intervalo especificado. 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, se agrega información sobre el mismo 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 computadoras (por ejemplo, impresoras y routers).

Para que este método de sondeo funcione, debe haber un servicio de DNS local correctamente configurado. El servicio debe tener una zona de búsqueda inversa. Si no se ha configurado tal zona, el sondeo de subredes IP no dará resultados. La zona de búsqueda inversa se mantiene automáticamente en redes con Active Directory. Sin embargo, en tales redes, el sondeo de subredes IP no brinda 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, para determinar qué intervalos IP se deben sondear, Kaspersky Security Center Cloud Console examina la configuración de red del dispositivo que actúa como punto de distribución y que se utiliza para realizar los sondeos. Si la dirección de este dispositivo es 192.168.0.1 y su 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 para sondear. En este caso, Kaspersky Security Center Cloud Console sondeará todas las direcciones comprendidas en el intervalo que va de 192.168.0.1 a 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 desee usar para sondear la red.

   Se abre la ventana de propiedades del punto de distribución.

4. Seleccione la sección **Sondeo de intervalos IP**.

5. Utilizando el interruptor **Habilitar sondeo de intervalos**, habilite o deshabilite el sondeo de intervalos IP.

6. Configure la programación de sondeo. De forma predeterminada, el sondeo de intervalos IP se ejecuta cada 420 minutos (7 horas).

7. Si es necesario, agregue otros intervalos IP para sondear o modifique los existentes.

   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.

Configurar un controlador de dominio Samba

Kaspersky Security Center Cloud Console es compatible con un controlador de dominio de Linux que se ejecuta solo en Samba 4.

Un controlador de dominio Samba admite las mismas extensiones de esquema que un controlador de dominio Microsoft Active Directory. Puede habilitar la compatibilidad total de un controlador de dominio Samba con un controlador de dominio Microsoft Active Directory utilizando la extensión de esquema Samba 4. Esta acción es opcional.

Recomendamos habilitar la compatibilidad total de un controlador de dominio Samba con un controlador de dominio Microsoft Active Directory. Esto asegurará la correcta interacción entre Kaspersky Security Center Cloud Console y el controlador de dominio de Samba.

Para habilitar la compatibilidad total de un controlador de dominio Samba con un controlador de dominio Microsoft Active Directory:

1. Ejecute el siguiente comando para utilizar la extensión de esquema RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Habilite la actualización del esquema en un controlador de dominio Samba. Para ello, agregue las siguientes líneas al archivo /etc/samba/smb.conf:

   ```
   dsdb:schema update allowed = true
   ```

   Si la actualización del esquema se completa con un error, deberá realizar una restauración completa del controlador de dominio que actúa como maestro de esquema.

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, para determinar qué intervalos IP se deben sondear, Kaspersky Security Center Cloud Console examina la configuración de red del dispositivo que actúa como punto de distribución y que se utiliza para realizar los sondeos. Si la dirección de este dispositivo es 192.168.0.1 y su 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 para sondear. En este caso, Kaspersky Security Center Cloud Console sondeará todas las direcciones comprendidas en el intervalo que va de 192.168.0.1 a 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 desee usar para sondear la red.

   Se abre la ventana de propiedades del punto de distribución.

4. Seleccione la sección **Sondeo de intervalos IP**.

5. Para agregar un nuevo intervalo IP, haga clic en el botón **Agregar**.

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 intervalo 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 (h)**

     Al configurar este ajuste, asegúrese de que el valor supere el intervalo de sondeo establecido en la programación de sondeos. Si la función de sondeo no verifica que una dirección IP se encuentra activa durante el tiempo de vigencia de las direcciones IP, la dirección se elimina automáticamente de los resultados del sondeo. Los resultados de los sondeos tienen una vida útil por defecto de veinticuatro horas; esto se debe a que las direcciones IP dinámicas (las que se asignan mediante el protocolo de configuración dinámica de hosts, DHCP) cambian cada veinticuatro horas.

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 de Kaspersky Security Center Cloud Console cumple las siguientes funciones:

- 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, membresía 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.

- Define los derechos de acceso a los dispositivos y a los 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. Cuando los puntos de distribución están repartidos del mejor modo posible, se reduce el volumen de tráfico en la red de la organización.

Dependiendo del organigrama de la organización y de la topología de la red, pueden aplicarse las siguientes configuraciones estándares a la estructura de grupos de administración:

- Oficina única
- Varias oficinas remotas pequeñas

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

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 siguientes tablas 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 deshabilitado.

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 no hay un punto de distribución disponible, actualice las bases de datos, los módulos de software y las aplicaciones de Kaspersky de forma manual 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:

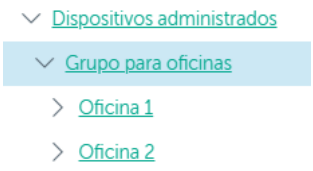
- Armar la estructura de grupos de administración tomando en cuenta la topología de la red. No es necesario que la estructura de grupos de administración refleje con absoluta precisión la topología de la red. Es suficiente con que haya coincidencia entre las partes independientes de la red y ciertos 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 original en cada una de las partes independientes de la red; por ejemplo, para el grupo **Dispositivos administrados**. Todos los puntos de distribución estarán en un mismo nivel y tendrán el mismo alcance (todos abarcarán la totalidad de dispositivos conectados a la red de la organización). Cada Agente de red se conectará al punto de distribución hacia el que exista la ruta más corta. La ruta a un punto de distribución se puede determinar con la utilidad tracert.

Configuración estándar de puntos de distribución: varias oficinas remotas pequeñas

Esta configuración estándar contempla la existencia de varias pequeñas oficinas remotas, que pueden comunicarse con una oficina central a través de Internet. Cada oficina remota está ubicada detrás de una pasarela NAT; debido a ello, las oficinas remotas están aisladas las unas de las otras y no se pueden conectar entre sí.

La configuración se debe ver reflejada en la estructura de grupos de administración: debe crearse un grupo de administración independiente para cada oficina remota (los grupos **Oficina 1** y **Oficina 2** en la siguiente imagen).



Oficinas remotas incluidas en la estructura de grupos de administración

Cada grupo de administración correspondiente a una oficina debe tener asignados uno o más puntos de distribución. Los puntos de distribución deben ser dispositivos que se encuentren en la oficina remota y deben tener una cantidad suficiente de espacio libre en disco. Los dispositivos incluidos en el grupo **Oficina 1** accederán a los puntos de distribución asignados al grupo de administración **Oficina 1**, por ejemplo.

Cuando hay usuarios que utilizan una computadora portátil para trabajar físicamente en más de una oficina, resulta necesario designar, junto con los puntos de distribución existentes, dos o más dispositivos en cada oficina remota para que actúen como puntos de distribución de un grupo de administración ubicado en un nivel superior (el grupo llamado **Grupo para oficinas** en la imagen anterior).

Ejemplo: Una computadora portátil incluida en el grupo de administración **Oficina 1** se traslada físicamente a la oficina que corresponde al grupo de administración **Oficina 2**. Luego del traslado, el Agente de red de la computadora portátil intenta acceder a los puntos de distribución asignados al grupo **Oficina 1**, pero esos puntos de distribución no están disponibles. Tras ello, el Agente de red intenta acceder a los puntos de distribución asignados al **Grupo para oficinas**. Como las oficinas remotas están aisladas entre sí, los intentos de acceder a los puntos de distribución asignados al grupo de administración **Grupo para oficinas** solo tendrán éxito cuando el Agente de red intente acceder a los puntos de distribución del grupo **Oficina 2**. Así, la computadora portátil permanecerá en el grupo de administración correspondiente a su oficina inicial, pero usará el punto de distribución de la oficina en la que se encuentre físicamente.

Designación manual de puntos de distribución

Kaspersky Security Center Cloud Console permite elegir manualmente los dispositivos que actuarán como puntos de distribución. Le recomendamos que calcule la cantidad y la configuración de los puntos de distribución requeridos 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 **Agregar**.

El punto de distribución agregado aparecerá en la lista de puntos de distribución, en la sección **Puntos de distribución**.

7. En la lista de puntos de distribución, seleccione el punto de distribución que acaba de agregar 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 y los dispositivos cliente:

     - **Puerto SSL**

       El número del puerto SSL que se usará para establecer una conexión cifrada con SSL entre el punto de distribución y los dispositivos cliente.

       De manera predeterminada, se utiliza el puerto 13000.

     - **Utilizar multidifusión**

       Si habilita esta opción, se utilizará la multidifusión IP para distribuir automáticamente los paquetes de instalación a los dispositivos cliente del grupo.

       Cuando necesite instalar una aplicación en un grupo de dispositivos cliente utilizando un paquete de instalación, la multidifusión IP ayudará a que el proceso se complete más rápidamente. Sin embargo, cuando se necesita instalar una aplicación en un único dispositivo cliente, la multidifusión hace que el tiempo de instalación aumente.

     - **Dirección de multidifusión IP**

       La dirección IP que se utilizará para la multidifusión. Puede usar cualquier dirección IP del intervalo 224.0.0.0-239.255.255.255

       De manera predeterminada, Kaspersky Security Center Cloud Console asigna automáticamente una dirección de multidifusión IP única tomada de este intervalo.

     - **Puerto para la multidifusión IP**

       Número del puerto que se usará para la multidifusión IP.

       El puerto por defecto es el 15001. De forma predeterminada, si el dispositivo que tiene instalado el Servidor de administración es, además, el punto de distribución designado, se usará el puerto 13001 para las conexiones SSL.

     - **Desplegar actualizaciones**

Las actualizaciones se distribuirán a los dispositivos administrados desde las siguientes fuentes:

- si deja esta opción habilitada: el presente punto de distribución;
- si deshabilita esta opción: otros puntos de distribución, el Servidor de administración o los servidores de actualizaciones de Kaspersky.

Si utiliza puntos de distribución para distribuir las actualizaciones, reducirá el número de descargas y verá una merma en el volumen de tráfico. Además, al distribuir la carga entre los puntos de distribución, también logrará aminorar la carga del Servidor de administración. Puede calcular cuántos puntos de distribución necesitará en su red para reducir los volúmenes de tráfico y de carga.

Si deshabilita esta opción, el número de descargas de actualizaciones y la carga del Servidor de administración podrían aumentar. Esta opción está activada de forma predeterminada.

- **Desplegar paquetes de instalación**

  Los paquetes de instalación se distribuirán a los dispositivos administrados desde las siguientes fuentes:

  - si deja esta opción habilitada: el presente punto de distribución;
  - si deshabilita esta opción: otros puntos de distribución, el Servidor de administración o los servidores de actualizaciones de Kaspersky.

  Si utiliza puntos de distribución para desplegar los paquetes de instalación, reducirá el número de descargas y verá una merma en el volumen de tráfico. Además, al distribuir la carga entre los puntos de distribución, también logrará aminorar la carga del Servidor de administración. Puede calcular cuántos puntos de distribución necesitará en su red para reducir los volúmenes de tráfico y de carga.

  Si deshabilita esta opción, el número de descargas de paquetes de instalación y la carga del Servidor de administración podrían aumentar. Esta opción está activada de forma predeterminada.

- **Ejecutar servidor push**

  En Kaspersky Security Center Cloud Console, un punto de distribución puede funcionar como un 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 habilitar el servidor push. Si tiene varios puntos de distribución asignados para el mismo grupo de administración, puede habilitar el servidor push en cada uno de los puntos de distribución. En este caso, el Servidor de administración equilibra la carga entre los puntos de distribución.

- **Puerto del servidor push**

  El número de puerto para el servidor push. Puede especificar el número de cualquier puerto que esté desocupado.

- En la sección **Alcance**, especifique el alcance al que el punto de distribución distribuirá las actualizaciones (grupos de administración y/o ubicación de red).

  Para que un dispositivo pueda determinar su ubicación de red, debe tener un sistema operativo Windows. No se puede determinar la ubicación de red de dispositivos con otros sistemas operativos.

- En la sección **Proxy de KSN**, puede configurar la aplicación para que utilice el punto de distribución para reenviar las solicitudes KSN desde los dispositivos administrados.

  Habilitar el proxy de KSN en el lado del punto de distribución

  El servicio de proxy de KSN se ejecuta en el dispositivo que se utiliza como punto de distribución. Utilice esta función para redistribuir y optimizar el tráfico de la red.

  Esta característica no estará disponible si el dispositivo que actúa como punto de distribución utiliza un sistema operativo 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 forma predeterminada. Esta opción solo se activa si la opción **Acepto utilizar 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 utiliza un punto de distribución de Linux con la versión 15 del Agente de red instalada, puede sondear solo los dominios de Active Directory para los cuales especifique la dirección y las credenciales de usuario. El sondeo del dominio de Active Directory actual y el bosque de dominios de Active Directory no está disponibles.

Puede habilitar el descubrimiento de dispositivos para los controladores de dominio.

Si selecciona la opción **Habilitar el sondeo de controladores de dominio**, puede seleccionar controladores de dominio para el sondeo y también especificar el programa de sondeo para ellos.

Si utiliza un punto de distribución de Linux, en la sección **Sondear dominios específicos**, haga clic en **Agregar** y luego especifique la dirección y las credenciales de usuario del controlador de dominio.

Si utiliza un punto de distribución de Windows, puede seleccionar una de las siguientes opciones:

- **Sondear dominio actual**
- **Sondear bosque de dominio entero**
- **Sondear dominios específicos**

- Sondeo de intervalos IP

  Puede habilitar el descubrimiento de dispositivos en intervalos IPv4 y en redes IPv6.

  Tras habilitar la opción **Habilitar sondeo de intervalos**, podrá agregar los intervalos que se sondearán y definir una programación para los sondeos. Puede agregar intervalos IP a la lista de los intervalos analizados.

  Si habilita la opción **Usar Zeroconf para el sondeo de redes IPv6**, el punto de distribución sondeará la red IPv6 automáticamente utilizando Zeroconf, una *tecnología para crear redes sin configuración*. En ese caso, el punto de distribución sondeará la red completa; el sondeo no estará limitado a los intervalos IP que especifique. La opción **Usar Zeroconf para el sondeo de redes IPv6** está disponible si el punto de distribución ejecuta Linux. Para usar el sondeo de Zeroconf IPv6, debe instalar la utilidad avahi-browse en el punto de distribución.

- En la sección **Avanzado**, especifique la carpeta en la que el punto de distribución guardará los datos distribuidos:

  - Usar carpeta predeterminada

    Si selecciona esta opción, la aplicación utilizará la carpeta de instalación del Agente de red en el punto de distribución.

  - Usar carpeta especificada

    Si selecciona esta opción, especifique la ruta a la carpeta en el campo que verá debajo. Puede usar una carpeta local del punto de distribución o una carpeta de otro dispositivo conectado a la red corporativa.

    La cuenta de usuario que se utilice para ejecutar el Agente de red en el punto de distribución deberá tener acceso de lectura y escritura a la carpeta especificada.

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 de grupos de administración, seleccione el grupo de administración para el que desee ver la lista de puntos de distribución.
3. Haga clic en la pestaña **Puntos de distribución**.
4. Utilice el botón **Asignar** para agregar nuevos puntos de distribución al grupo de administración y el botón **Desasignar** para quitar los puntos de distribución asignados.

   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 un 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 habilitar el servidor push. Si tiene varios puntos de distribución asignados para el mismo grupo de administración, puede habilitar el servidor push en cada uno de los puntos de distribución. En este caso, el Servidor de administración equilibra la carga entre los puntos de distribución.

Puede usar puntos de distribución como servidores push para asegurarse de que haya una conectividad continua entre un dispositivo administrado y el Servidor de administración. Se necesita conectividad continua para algunas operaciones, como ejecutar y detener tareas locales, recibir estadísticas para una aplicación administrada o crear un túnel. Si utiliza un punto de distribución como servidor push, no es necesario que envíe 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 desee usar como servidor push.
4. En la lista de propiedades del punto de distribución seleccionado, vaya a la sección **General** y, a continuación, habilite la opción **Ejecutar servidor push**.

   El campo de entrada **Puerto del servidor push** estará disponible.
5. En el campo de entrada **Puerto del servidor push**, especifique el puerto del punto de distribución que los dispositivos cliente usarán para conectarse. 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 exclusiones del Firewall de Microsoft Windows.

6. Haga clic en **Aceptar** para salir de la ventana de propiedades del punto de distribución y, a continuación, haga clic en **Guardar** para aplicar los cambios.

   Después de habilitar la opción **Ejecutar servidor push**, la opción **No desconectar del Servidor de administración** se habilita 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 de configuración de la directiva del Agente de red.

8. Vaya a **Conectividad** → **Red** y, a continuación, habilite la opción **Usar el punto de distribución para forzar la conexión con el Servidor de administración**. Bloquee esta opción.

9. Además, en la subsección **Red**, puede deshabilitar 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 UPD.

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 usa servidores push, Kaspersky Security Center Cloud Console no proporciona conectividad continua entre los dispositivos administrados y el Servidor de administración. Los Agentes de red en los dispositivos administrados periódicamente establecen conexiones y se sincronizan con el Servidor de administración. El intervalo entre esas sesiones de sincronización se define en una directiva del Agente de red. Si se requiere una sincronización temprana, el Servidor de administración (o un punto de distribución, si está en uso) envía un paquete de red firmado a través de una red IPv4 o IPv6 al puerto UDP del Agente de red. El puerto por defecto es el 15000. Si ninguna conexión a través de UDP es posible entre el Servidor de administración y un dispositivo administrado, la sincronización se ejecutará en la siguiente conexión regular del Agente de red al Servidor de administración dentro del intervalo de sincronización.

Algunas operaciones no se pueden realizar sin una conexión temprana entre el Agente de red y el Servidor de administración, como ejecutar y detener tareas locales, recibir estadísticas para una aplicación administrada o crear un túnel. Para resolver este problema, si no usa servidores push, puede usar la opción **No desconectar del Servidor de administración** para garantizar que haya una conectividad continua entre el dispositivo administrado y el Servidor de administración.

Para proporcionar conexión continua entre un dispositivo administrado y el Servidor de administración:

1. 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 con el que desea proporcionar conectividad continua.

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 pertinente.

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

En un primer momento, la jerarquía de grupos de administración contiene un único grupo de administración, llamado **Dispositivos administrados**. Al crear una jerarquía de grupos de administración, puede agregar dispositivos y máquinas virtuales al grupo **Dispositivos administrados** y agregar subgrupos. La ventana de propiedades de cada grupo de administración contiene datos sobre las directivas, las tareas y los dispositivos vinculados a ese grupo.

Para crear un grupo de administración:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. Active la casilla de verificación ubicada junto al grupo de administración al que pertenecerá el subgrupo que desea crear.
3. Haga clic en el botón **Agregar**.
4. Escriba un nombre para el nuevo grupo de administración.
5. Haga clic en el botón **Agregar**.

En la jerarquía de grupos de administración, aparecerá un nuevo grupo de administración con el nombre que haya indicado.

La aplicación permite crear una jerarquía de grupos de administración basada en la estructura de Active Directory o 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.

Crear reglas de movimiento de dispositivos

Puede configurar reglas de movimiento de dispositivos; es decir, reglas que asignan automáticamente dispositivos a grupos de administración.

Para crear una regla de movimiento:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Reglas de movimiento**.
2. Haga clic en **Agregar**.
3. En la ventana que se abre, especifique la siguiente información en la pestaña **General**:

- **Nombre de la regla**

  Ingrese un nombre para la nueva regla.

  Cuando se copia una regla, la regla nueva recibe el nombre de la regla de origen, con el agregado de un índice numérico entre paréntesis, como (1).

- **Grupo de administración**

  Seleccione el grupo de administración al que se moverán automáticamente los dispositivos.

- **Regla activa**

  Si esta opción está habilitada, la regla se habilitará y empezará a operar en cuanto la guarde.

  Si esta opción está deshabilitada, la regla se creará, pero no se activará. No entrará en funcionamiento hasta que habilite esta opción.

- **Mover solo los dispositivos que no pertenezcan a un grupo de administración**

  Si esta opción está habilitada, solo los dispositivos no asignados se moverán al grupo seleccionado.

  Si esta opción está deshabilitada, tanto los dispositivos no asignados como los dispositivos que ya pertenezcan a otro grupo de administración se moverán al grupo seleccionado.

- **Aplicar regla**

Puede seleccionar una de las siguientes opciones:

- **Ejecutar una vez por dispositivo**

  La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados.

- **Ejecutar una vez por dispositivo y luego cada vez que se reinstale el Agente de red**

  La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados; tras esa primera aplicación, la regla se aplicará solo cuando el Agente de red se reinstale en esos dispositivos.

- **Aplicar esta regla continuamente**

  La regla se aplicará siguiendo una programación definida automáticamente por el Servidor de administración (generalmente, una vez cada varias horas).

4. En la pestaña **Condiciones de la regla**, especifique al menos un criterio por el cual los dispositivos se mueven a un grupo de administración.

5. Haga clic en **Guardar**.

Se crea la regla de movimiento. La nueva regla aparece en la lista de reglas de movimiento.

Cuanto más alta sea la posición en la lista, mayor será la prioridad de la regla. Para aumentar o reducir la prioridad de una regla de movimiento, mueva la regla en la lista hacia arriba o hacia abajo, respectivamente, con el mouse.

Si se selecciona la opción **Aplicar esta regla continuamente**, la regla de movimiento se aplica independientemente de la configuración de prioridad. Esas reglas se aplican de acuerdo con la programación que el Servidor de administración configura automáticamente.

Si los atributos de dispositivo cumplen con las condiciones de varias reglas, el dispositivo se mueve al grupo de destino de la regla con la prioridad más alta (es decir, la que tiene la clasificación más alta en la lista de reglas).

Copiar reglas de movimiento de dispositivos

Puede copiar sus reglas de movimiento de dispositivos si, por ejemplo, desea tener varias reglas de movimiento idénticas para diferentes grupos de administración de destino.

Para copiar una regla de movimiento existente:

1. Realice una de las siguientes acciones:

   - En el menú principal, vaya a **Activos (dispositivos)** → **Reglas de movimiento**.

   - En el menú principal, vaya a **Descubrimiento y despliegue** → **Despliegue y asignación** → **Reglas de movimiento**.

   Se muestra la lista de reglas de movimiento.

2. Marque la casilla ubicada junto a la regla que desee copiar.

3. Haga clic en **Copiar**.

4. En la ventana que se abre, cambie la siguiente información en la pestaña **General** (si desea copiar la regla sin modificar su configuración, no haga ningún cambio):

   - Nombre de la regla

     Ingrese un nombre para la nueva regla.

     Cuando se copia una regla, la regla nueva recibe el nombre de la regla de origen, con el agregado de un índice numérico entre paréntesis, como (1).

   - Grupo de administración

     Seleccione el grupo de administración al que se moverán automáticamente los dispositivos.

   - Regla activa

     Si esta opción está habilitada, la regla se habilitará y empezará a operar en cuanto la guarde.

     Si esta opción está deshabilitada, la regla se creará, pero no se activará. No entrará en funcionamiento hasta que habilite esta opción.

   - Mover solo los dispositivos que no pertenezcan a un grupo de administración

     Si esta opción está habilitada, solo los dispositivos no asignados se moverán al grupo seleccionado.

     Si esta opción está deshabilitada, tanto los dispositivos no asignados como los dispositivos que ya pertenezcan a otro grupo de administración se moverán al grupo seleccionado.

   - Aplicar regla

     Puede seleccionar una de las siguientes opciones:

     - **Ejecutar una vez por dispositivo**

       La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados.

     - **Ejecutar una vez por dispositivo y luego cada vez que se reinstale el Agente de red**

       La regla se aplicará una vez por cada dispositivo que reúna los criterios especificados; tras esa primera aplicación, la regla se aplicará solo cuando el Agente de red se reinstale en esos dispositivos.

     - **Aplicar esta regla continuamente**

       La regla se aplicará siguiendo una programación definida automáticamente por el Servidor de administración (generalmente, una vez cada varias horas).

5. En la pestaña **Condiciones de la regla**, especifique al menos un criterio para los dispositivos que desea que se muevan automáticamente.

6. Haga clic en **Guardar**.

Se crea la nueva regla de movimiento. La nueva regla aparece en la lista de reglas de movimiento.

Condiciones para una 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 la regla** las condiciones mover los dispositivos. Para determinar qué dispositivos mover, puede utilizar los siguientes criterios:

- Etiquetas asignadas a los dispositivos cliente.
- Parámetros de red. Por ejemplo, puede mover dispositivos con direcciones IP de un rango específico.
- Aplicaciones administradas instaladas en dispositivos cliente, por ejemplo, Agente de red o Servidor de administración.
- Máquinas virtuales, que son los dispositivos cliente.
- Información sobre la unidad organizativa (OU) de Active Directory con los dispositivos cliente.
- Información sobre un segmento de nube con los dispositivos cliente.

A continuación, puede encontrar la descripción sobre cómo especificar esta información en una regla de movimiento de dispositivos.

Si especifica varias condiciones en la regla, se usa el operador lógico AND y todas las condiciones se aplican al mismo tiempo. Si no selecciona ninguna opción o deja algunos campos en blanco, dichas condiciones no se aplican.

Pestaña Etiquetas

En esta pestaña, puede configurar una búsqueda del dispositivo según las etiquetas para dispositivos que se añadieron anteriormente a las descripciones de los dispositivos administrados: Para hacerlo, seleccione las etiquetas pertinentes. Además, puede habilitar las siguientes opciones:

- **Aplicar a los dispositivos que no tengan las etiquetas especificadas**

  Si esta opción está habilitada, todos los dispositivos con las etiquetas especificadas se excluyen de una regla de movimiento de dispositivos. Si esta opción está deshabilitada, la regla de movimiento de dispositivos se aplica a los dispositivos con todas las etiquetas seleccionadas.

  Esta opción está deshabilitada de forma predeterminada.

- **Aplicar si coincide al menos una etiqueta especificada**

  Si esta opción está habilitada, se aplica una regla de movimiento de dispositivos a los dispositivos cliente con al menos una de las etiquetas seleccionadas. Si esta opción está deshabilitada, la regla de movimiento de dispositivos se aplica a los dispositivos con todas las etiquetas seleccionadas.

  Esta opción está deshabilitada de forma predeterminada.

Pestaña Red

En esta pestaña, puede especificar los datos de red de los dispositivos a los que atañe una regla de movimiento de dispositivos:

- **Nombre del dispositivo en la red de Windows**

  Nombre de red de Windows (nombre NetBIOS) del dispositivo, o la dirección IPv4 o IPv6.

- **Dominio de Windows**

  Una regla de movimiento de dispositivos se aplica a todos los dispositivos incluidos en el dominio de Windows especificado.

- **Nombre DNS del dispositivo**

  Nombre de dominio DNS del dispositivo cliente que desea mover. Complete este campo si su red incluye un servidor DNS.

  Si la intercalación con diferenciación entre mayúsculas y minúsculas está configurada para la base de datos utilizada para Kaspersky Security Center Cloud Console, respete las mayúsculas y minúsculas cuando ingrese el nombre DNS de un dispositivo. De lo contrario, la regla de movimiento de dispositivos no funcionará.

- **Dominio DNS**

  Una regla de movimiento de dispositivos se aplica a todos los dispositivos incluidos en el sufijo DNS principal especificado. Complete este campo si su red incluye un servidor DNS.

- **Intervalo IP**

  Si habilita esta opción, podrá ingresar las direcciones IP inicial y final del intervalo IP en el que deberán estar incluidos los dispositivos pertinentes.

  Esta opción está deshabilitada de forma predeterminada.

- **Dirección IP para establecer conexión con el Servidor de administración**

  Si esta opción está habilitada, puede configurar las direcciones IP mediante las cuales los dispositivos cliente se conectan al Servidor de administración. Para hacerlo, especifique el rango de IP que incluye todas las direcciones IP necesarias.

  Esta opción está deshabilitada de forma predeterminada.

- **El dispositivo se encuentra en este intervalo IP**

  Si esta opción está activada, puede seleccionar un rango de IP que haya agregado previamente en la sección **Intervalos IP**. Los dispositivos relevantes deben estar incluidos en el rango IP seleccionado.

  Esta opción está deshabilitada de forma predeterminada.

- **Perfil de conexión cambiado**

Seleccione uno de los siguientes valores:

- **Sí**. Una regla de movimiento de dispositivos solo se aplica a los dispositivos cliente con un perfil de conexión modificado.
- **No**. La regla de movimiento de dispositivos solo se aplica a los dispositivos cliente cuyo perfil de conexión no cambió.
- **Ningún valor seleccionado**. La condición no se aplica.

- Administrado por un Servidor de administración diferente

  Seleccione uno de los siguientes valores:

  - **Sí**. Una regla de movimiento de dispositivos solo se aplica a los dispositivos cliente administrados por otros Servidores de administración. Estos servidores son diferentes del servidor en el que configura la regla de movimiento de dispositivos.
  - **No**. La regla de movimiento de dispositivos solo se aplica a los dispositivos cliente administrados por el Servidor de administración actual.
  - **Ningún valor seleccionado**. La condición no se aplica.

Pestaña Aplicaciones

En esta pestaña, puede configurar una regla de movimiento de dispositivos basada en las aplicaciones administradas y los sistemas operativos instalados en los dispositivos cliente:

- Agente de red instalado

  Seleccione uno de los siguientes valores:

  - **Sí**. Una regla de movimiento de dispositivos solo se aplica a los dispositivos cliente con el Agente de red instalado.
  - **No**. La regla de movimiento de dispositivos solo se aplica a los dispositivos cliente en los que el Agente de red no está instalado.
  - **Ningún valor seleccionado**. La condición no se aplica.

- Aplicaciones

  Especifique qué aplicaciones administradas deben instalarse en los dispositivos cliente, de modo que se aplique una regla de movimiento de dispositivos a estos dispositivos. Por ejemplo, puede seleccionar **Agente de red de Kaspersky Security Center 15.3** 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.

- Arquitectura del sistema operativo

  Puede seleccionar dispositivos cliente según el tamaño de bits del sistema operativo. En el bloque **Arquitectura del sistema operativo**, puede seleccionar uno de los siguientes valores:

  - **Desconocido**
  - **x86**
  - **AMD64**
  - **IA64**

  Para comprobar el tamaño de bits del sistema operativo de los dispositivos cliente:

  1. En el menú principal, vaya a la sección **Activos (dispositivos)** → **Dispositivos administrados**.
  2. Haga clic en el botón **Configuración de las columnas** ( ) a la derecha.
  3. Seleccione la opción **Arquitectura del sistema operativo**, y haga clic en el botón **Guardar**.

     Después, se muestra el tamaño de bits del sistema operativo para cada dispositivo administrado.

- Versión del Service Pack del sistema operativo

  En este campo, puede especificar la versión del paquete de su sistema operativo (en formato *X.Y.*), que determinará cómo aplicar la regla de migración a su dispositivo. De manera predeterminada, no hay una versión definida.

- Certificado de usuario

  Seleccione uno de los siguientes valores:

  - **Instalado**. Una regla de movimiento de dispositivos solo se aplica a dispositivos móviles con un certificado para dispositivos móviles.
  - **Sin instalar**. La regla de movimiento de dispositivos solo se aplica a dispositivos móviles sin un certificado para dispositivos móviles.
  - **Ningún valor seleccionado**. La condición no se aplica.

- Compilación del sistema operativo

Este parámetro solo es válido para sistemas operativos Windows.

Puede indicar si el número de compilación del sistema operativo seleccionado deberá ser igual, anterior o posterior al valor introducido. También puede configurar la búsqueda de una regla de movimiento para todos los números de compilación, excepto el especificado.

- Número de versión del sistema operativo

Este parámetro solo es válido para sistemas operativos Windows.

Puede especificar si el sistema operativo seleccionado debe tener un número de versión igual, anterior o posterior. También puede configurar una regla de movimiento de dispositivos para todos los números de versión excepto el especificado.

Pestaña Máquinas virtuales

En esta pestaña puede configurar la búsqueda de dispositivos según sean dispositivos virtuales o parte de la infraestructura de escritorio virtual (VDI):

- Esta es una máquina virtual

En la lista desplegable se puede seleccionar lo siguiente:

- **N/D**. La condición no se aplica.
- **No**. Mover dispositivos que no son máquinas virtuales.
- **Sí**. Mover dispositivos que son máquinas virtuales.

- **Tipo de máquina virtual**
- Parte de la infraestructura de escritorio virtual

En la lista desplegable se puede seleccionar lo siguiente:

- **N/D**. La condición no se aplica.
- **No**. Mover dispositivos que no forman parte de la VDI.
- **Sí**. Mover de dispositivos que son parte de la VDI.

Pestaña Controlador de dominio

En esta pestaña, puede especificar que es necesario mover los dispositivos incluidos en la unidad organizativa del dominio. También puede mover dispositivos de todas las unidades organizativas secundarias de la unidad organizativa del dominio especificado:

- El dispositivo está incluido en la siguiente unidad organizativa

  Si esta opción está habilitada, se aplica una regla de movimiento de dispositivos a los dispositivos de la unidad organizativa de Active Directory especificados en la lista que hay debajo de la opción.

  Esta opción está deshabilitada de forma predeterminada.

- Incluir unidades organizativas secundarias

  Si habilita esta opción, la selección incluirá los dispositivos de todas las unidades organizativas secundarias de la unidad organizativa de Active Directory especificada.

  Esta opción está deshabilitada de forma predeterminada.

- **Mover los dispositivos de unidades secundarias a subgrupos correspondientes**
- **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados**
- **Eliminar subgrupos no presentes en el dominio**
- Incluir el dispositivo en el siguiente grupo de seguridad de dominio

  Si esta opción está habilitada, se aplica una regla de movimiento de dispositivos a los dispositivos de la unidad organizativa de Active Directory especificados en la lista que hay debajo de la opción.

  Esta opción está deshabilitada de forma predeterminada.

Pestaña Segmentos de nube

En esta pestaña, puede especificar que es necesario mover los dispositivos que pertenecen a segmentos de la nube específicos:

- El dispositivo se encuentra en un segmento de la nube

  Si selecciona esta opción, una regla de movimiento de dispositivos se aplica a los dispositivos cliente que pertenecen a un segmento de la nube. Puede seleccionar el segmento de nube requerido hasta una subred en la lista que hay debajo de la opción.

  La opción está desactivada de forma predeterminada.

- Incluir objetos secundarios

  Si selecciona esta opción, se aplica una regla de movimiento de dispositivos no solo al segmento de nube seleccionado, sino también a los objetos secundarios de este segmento.

  La opción está desactivada de forma predeterminada.

- **Mover los dispositivos de objetos anidados a subgrupos correspondientes**
- **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados**
- **Eliminar subgrupos para los que no se encuentre coincidencia en los segmentos de nube**
- Dispositivo encontrado mediante API

La lista desplegable le permite operar con el hecho de que el dispositivo pueda detectarse con las herramientas provistas por una API.

- **AWS**. El dispositivo se descubre mediante la API de AWS, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de AWS.
- **Azure**. El dispositivo se descubre mediante la API de Azure, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Azure.
- **Google Cloud.** El dispositivo se descubre utilizando la API de Google, es decir, el dispositivo está en el entorno de Google Cloud.
- **No**. El dispositivo no se puede detectar con la API de AWS, Azure o Google (o bien el dispositivo no se encuentra en el entorno de nube, o bien sí está en el entorno de nube, pero, por algún motivo, no se lo puede detectar con una API).
- **Ningún valor.** Esta condición no se aplica.

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. Seleccione el grupo de administración al que desea agregar los dispositivos:
   - Para el grupo root:

     En este caso, puede avanzar al próximo 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.

     Verá la ruta al grupo seleccionado en la parte superior de la página. Si es necesario, puede hacer clic en un vínculo con el nombre del grupo de administración para ir al grupo. De forma predeterminada, el último vínculo de la ruta se encuentra inactivo.
3. Haga clic en el botón **Agregar 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 **Agregar dispositivos** y luego elija los dispositivos de una de las siguientes maneras:
  - Seleccione los dispositivos de la lista de dispositivos detectados por el Servidor de administración.
  - Especifique las direcciones IP de los dispositivos o un intervalo de direcciones IP.
  - Especifique los nombres NetBIOS o los nombres DNS de los dispositivos.

    El campo con el nombre del dispositivo no debe contener espacios en blanco, caracteres de retroceso ni ninguno de los siguientes caracteres prohibidos: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

- Haga clic en el botón **Importar dispositivos desde archivo** para importar una lista de dispositivos desde un archivo .txt. Utilice una línea diferente para la dirección o el nombre de cada dispositivo.

  El archivo no debe contener espacios en blanco, caracteres de retroceso ni ninguno de 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 procesará la lista de dispositivos y mostrará el resultado. Los dispositivos que se procesen correctamente se agregarán al grupo de administración y aparecerán en la lista de dispositivos con nombres generados por el Servidor de administración.

Mover dispositivos o clústeres a un grupo de administración en forma manual

Puede mover dispositivos de un grupo de administración a otro, o del grupo de dispositivos no asignados a un grupo de administración.

También puede mover clústeres o conjuntos de servidores de un grupo de administración a otro. Cuando mueve un clúster o un conjunto de servidores a otro grupo, todos sus nodos se mueven con él, porque un clúster y cualquiera de sus nodos siempre pertenecen al mismo grupo de administración. Cuando selecciona un solo nodo de clúster en la pestaña **Dispositivos**, el botón **Mover a un grupo** deja de estar disponible.

Para mover uno o varios dispositivos o clústeres a un grupo de administración seleccionado:

1. Abra el grupo de administración al que pertenezcan los dispositivos que desee mover. Para ello, realice una de las siguientes acciones:
   - Para abrir un grupo de administración, en el menú principal, vaya a **Activos (dispositivos)** → **Grupos** → **<nombre del grupo>** → **Dispositivos administrados**.
   - Para abrir el grupo **Dispositivos no asignados**, en el menú principal, vaya a **Descubrimiento y despliegue** → **Dispositivos no asignados**.

2. Si el grupo de administración contiene clústeres o conjuntos de servidores, la sección **Dispositivos administrados** se divide en dos pestañas: **Dispositivos** y **Clústeres y conjuntos de servidores** Abra la pestaña del objeto que desea mover.

3. Active las casillas ubicadas junto a los dispositivos o clústeres que desee mover a otro grupo.

4. Haga clic en el botón **Mover a un grupo**.

5. En la jerarquía de grupos de administración, marque la casilla ubicada junto al grupo de administración al que desee mover los dispositivos o clústeres seleccionados.

6. Haga clic en el botón **Mover**.

Los dispositivos o clústeres seleccionados se moverán al grupo de administración seleccionado.

Configuración de reglas de retención para dispositivos no asignados

Una vez finalizado el sondeo de la red de Windows, los dispositivos descubiertos se colocan en subgrupos del grupo de administración "Dispositivos no asignados". Este grupo de administración se encuentra en **Descubrimiento y despliegue → Descubrimiento → Dominios de Windows**. El grupo primario es la carpeta **Dominios de Windows**. Dicha carpeta contiene grupos secundarios que llevan el nombre de los dominios y grupos de trabajo descubiertos durante el sondeo. El grupo primario también puede contener el grupo de administración de dispositivos móviles. Puede configurar las reglas de retención de dispositivos no asignados para el grupo primario y para cada uno de los grupos secundarios. Las reglas de retención no dependen de la configuración del descubrimiento de dispositivos y funcionan incluso si el descubrimiento de dispositivos está deshabilitado.

Las reglas de retención de dispositivos no afectan a los dispositivos que tienen una o más unidades cifradas con cifrado de disco completo. Dichos dispositivos no se eliminan automáticamente, solo puede hacerlo de forma manual. Si necesita eliminar un dispositivo con una unidad cifrada, primero descifre la unidad y luego elimine el dispositivo.

Para configurar las reglas de retención para dispositivos no asignados:

1. En el menú principal, vaya a **Descubrimiento y despliegue → Descubrimiento → Dominios de Windows**.

2. Realice una de las siguientes acciones:

   - Para configurar los ajustes del grupo primario, haga clic en el botón **Propiedades**.

     Se abrirá la ventana de propiedades del dominio de Windows.

   - Para configurar los ajustes de un grupo secundario, haga clic en su nombre.

     Se abrirá la ventana de propiedades del grupo secundario.

3. Defina los siguientes parámetros de configuración:

   - **Eliminar el dispositivo del grupo si ha estado inactivo por más de (días)**

     Si esta opción está habilitada, puede especificar el intervalo de tiempo que se deja pasar antes de que el dispositivo se elimine del grupo automáticamente. De forma predeterminada, esta opción se propaga a los grupos secundarios. El intervalo de tiempo por defecto es de 7 días.

     Esta opción está activada de forma predeterminada.

- **Heredar del grupo primario**

  Si esta opción está habilitada, el período de retención de dispositivos en el grupo seleccionado se heredará del grupo primario y no se podrá modificar.

  Esta opción solo está disponible para grupos secundarios.

  Esta opción está activada de forma predeterminada.

- **Forzar herencia en grupos secundarios**

  Los valores de configuración se propagarán a los grupos secundarios. Los ajustes correspondientes estarán bloqueados en las propiedades de esos grupos.

  Esta opción está deshabilitada de forma predeterminada.

4. Haga clic en el botón **Aceptar**.

Se guardarán y aplicarán los cambios.

Configurar la protección de la red

En esta sección, encontrará información sobre la configuración manual de tareas y directivas, sobre los roles de usuario y sobre la creación de una jerarquía de tareas y una estructura de grupos de administración.

Procedimiento: Configurar la protección de la red

El asistente de inicio rápido crea directivas y tareas con la configuración predeterminada. Esta configuración podría ser subóptima (o incluso inadmisible) para su organización. Por este motivo, recomendamos que modifique estas directivas y tareas predeterminadas y que, de ser necesario, cree otras directivas y tareas adicionales para su red.

Requisitos previos

Antes de comenzar, asegúrese de haber completado el escenario de configuración inicial de Kaspersky Security Center Cloud Console. Recuerde que el escenario implica usar el asistente de inicio rápido.

Cuando se utiliza el asistente de inicio rápido, 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
- Buscar vulnerabilidades y 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. Los enfoques se pueden combinar.

2. **Configurar tareas para administrar las aplicaciones de Kaspersky en forma remota**

   Revise las tareas creadas con el asistente de inicio rápido y modifique sus ajustes según corresponda.

   Instrucciones:

   - Configuración de la tarea de grupo para actualizar Kaspersky Endpoint Security
   - Crear la tarea *Buscar vulnerabilidades y actualizaciones requeridas*

   De ser necesario, cree tareas adicionales para administrar las aplicaciones de 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.

El enfoque centrado en el dispositivo permite que la configuración de una aplicación de seguridad varíe según las características del dispositivo administrado en el que se encuentra instalada. Es posible, por ejemplo, definir ajustes de configuración diferentes para dispositivos asignados a grupos de administración diferentes. Los dispositivos también pueden diferenciarse sobre la base de sus especificaciones de hardware o de su uso en Active Directory.

El enfoque centrado en el usuario permite configurar las aplicaciones de seguridad de maneras diferentes para roles de usuario diferentes. Puede crear una serie de roles de usuario, asignarlos a sus usuarios según las funciones que desempeñen en la empresa y luego crear configuraciones diferentes, que se apliquen a uno u otro dispositivo según el rol asignado al propietario del dispositivo. Imagine, por ejemplo, que una aplicación de Kaspersky debe estar configurada de un modo diferente si se encuentra instalada en el dispositivo de un contador o en el dispositivo de un especialista en RR. HH. Al implementar la administración de la seguridad centrada en el usuario, puede hacer que cada departamento (el de Contabilidad y el de Recursos Humanos) tenga su propio "juego de ajustes" para esa aplicación. El juego de ajustes determina qué valores de configuración pueden ser modificados por los usuarios y cuáles se imponen por la fuerza y solamente pueden ser modificados por el administrador.

El enfoque centrado en el usuario también permite configurar una aplicación de un modo específico para un usuario específico. Esto puede ser útil si hay un empleado con un rol único en la empresa o si se quieren supervisar los problemas de seguridad asociados a los dispositivos de una persona en particular. El rol de este empleado en particular podría determinar si la persona tendrá más o menos derechos para modificar los ajustes de la aplicación. Un administrador de sistemas que tenga a su cargo los dispositivos cliente de una oficina local podría necesitar más derechos que otros usuarios.

El enfoque centrado en el dispositivo y el enfoque centrado en el usuario pueden combinarse. Podría, por ejemplo, configurar una directiva de aplicación específica para cada uno de sus grupos de administración y, luego, podría crear perfiles de directivas que se apliquen a uno o más de los roles de usuario definidos en su empresa. Si hace esto, las directivas y los perfiles se aplicarán en el siguiente orden:

1. Se aplicarán las directivas creadas en el marco del enfoque centrado en el dispositivo.
2. Los perfiles modificarán las directivas siguiendo el orden de prioridad definido para los perfiles de directivas.
3. Los perfiles de directivas vinculados a los roles de usuario modificarán las directivas.

Configuración y propagación de directivas: enfoque centrado en el dispositivo

En esta sección se describe un proceso para configurar, de manera centralizada y tomando el dispositivo como eje, 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 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 se utiliza el asistente de inicio rápido para configurar la protección de la red, Kaspersky Security Center Cloud Console crea una directiva predeterminada para Kaspersky Endpoint Security para Windows. Si completó el proceso de configuración utilizando este asistente, no es necesario que cree una nueva directiva para esta aplicación. En cambio, puede simplemente configurar la directiva de Kaspersky Endpoint Security en forma manual.

   De manera predeterminada, cuando existe una estructura jerárquica de grupos de administración, los grupos de administración secundarios heredan las directivas del Servidor de administración principal. Puede forzar la herencia en los grupos secundarios para evitar todo riesgo de que los ajustes configurados en la directiva de nivel superior se modifiquen. Si desea que solo algunos de los ajustes se hereden por la fuerza, bloquee esos ajustes en la directiva de nivel superior. Los ajustes que queden desbloqueados se podrán modificar en las directivas de niveles inferiores. La jerarquía de directivas resultante le será de gran utilidad para administrar 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.

Para administrar la seguridad, considere también utilizar un enfoque centrado en el dispositivo, ya sea en reemplazo o como complemento de este enfoque centrado en el usuario. Obtenga 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 se utiliza el asistente de inicio rápido para configurar la protección de la red, Kaspersky Security Center Cloud Console crea una directiva predeterminada para Kaspersky Endpoint Security. Si completó el proceso de configuración utilizando este asistente, no es necesario que cree una nueva directiva para esta aplicación. En cambio, puede sencillamente configurar la directiva de Kaspersky Endpoint Security en forma manual.

De manera predeterminada, cuando existe una estructura jerárquica de grupos de administración, los grupos de administración secundarios heredan las directivas del Servidor de administración principal. Puede forzar la herencia en los grupos secundarios para evitar todo riesgo de que los ajustes configurados en la directiva de nivel superior se modifiquen. Si desea que solo algunos de los ajustes se hereden por la fuerza, bloquee esos ajustes en la directiva de nivel superior. Los ajustes que queden desbloqueados se podrán modificar en las directivas de niveles inferiores. 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 un rol de usuario para cada grupo de empleados que haya definido en el paso anterior o utilice los roles 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 cambiar el estado de la directiva y modificar los ajustes que controlan la herencia de sus valores de configuración:

- A través del bloque **Estado de la directiva**, puede seleccionar uno de los modos posibles para la 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 primaria**

Si habilita esta opción, la directiva heredará los valores de configuración definidos en la directiva del grupo de nivel superior. Estos valores, en consecuencia, estarán bloqueados.

Esta opción está activada de forma predeterminada.

- Forzar la herencia de configuración en las directivas secundarias

  Si habilita esta opción, cuando modifique la directiva y se apliquen los cambios, ocurrirá lo siguiente:

  - Los valores de configuración de la directiva se propagarán a las directivas de los subgrupos de administración (es decir, a las directivas secundarias).
  - En la ventana de propiedades de cada directiva secundaria, dentro del bloque **Herencia de configuración** de la sección **General**, se habilitará automáticamente la opción **Heredar configuración de la directiva primaria**.

  Habilitar esta opción hace que los ajustes de las directivas secundarias se bloqueen.

  Esta opción está deshabilitada de forma predeterminada.

Pestaña Configuración de eventos

Utilice esta pestaña para configurar ajustes relativos al registro de los eventos y a las notificaciones que se envían cuando ocurre un evento. Los eventos se organizan por nivel de importancia en las siguientes secciones de la pestaña **Configuración de eventos**:

- **error funcional**
- **Advertencia**
- **Información**

Cada sección contiene una lista con los distintos tipos de eventos y, junto a ellos, la cantidad de días por los que cada evento se deja almacenado, por defecto, en el Servidor de administración. Al hacer clic en el botón **Propiedades**, podrá especificar los parámetros del registro de eventos y las notificaciones de los eventos seleccionados en la lista. De forma predeterminada, todos los tipos de eventos están sujetos a los ajustes de notificación generales configurados para el Servidor de administración entero. 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 a través de los puntos de distribución

  Si habilita esta opción, los dispositivos cliente no descargarán sus actualizaciones directamente de los servidores de actualizaciones: las obtendrán únicamente de los puntos de distribución.

  Si no habilita esta opción, los dispositivos cliente podrán obtener sus actualizaciones de distintas fuentes (directamente de los servidores de actualizaciones o de una carpeta local o de red).

  Esta opción está deshabilitada de forma predeterminada.

- **Tamaño máximo de la cola de eventos, 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 forma predeterminada.

- **Evitar que el servicio del Agente de red se detenga o se elimine sin autorización e impedir cambios en su configuración**

  Cuando esta opción está habilitada, una vez que el Agente de red se encuentre instalado en un dispositivo administrado, no se lo podrá eliminar ni reconfigurar a menos que se tengan los privilegios necesarios. El servicio del Agente de red no se podrá detener. Esta opción no tiene efecto en los controladores de dominio.

  Habilite esta opción para proteger el Agente de red en estaciones de trabajo operadas con derechos de administrador local.

  Esta opción está deshabilitada de forma predeterminada.

- **Utilizar contraseña de desinstalación**

  Si activa esta opción y hace clic en el botón **Modificar**, podrá especificar la contraseña para la utilidad klmover y la desinstalación remota del Agente de red.

  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 forma predeterminada.

Repositorios

En la sección **Repositorios**, puede seleccionar los tipos de objetos sobre los que el Agente de red enviará detalles al Servidor de administración. La directiva del Agente de red podría impedirle modificar algunos ajustes de esta sección:

- **Detalles de las aplicaciones instaladas**
- Incluir información sobre parches

  Se enviará información al Servidor de administración sobre los parches de las aplicaciones instaladas en los dispositivos clientes. Si habilita esta opción, podría aumentar la carga del Servidor de administración y del sistema de administración de bases de datos (DBMS). También podría aumentar el volumen de la base de datos.

  Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

- Detalles de las actualizaciones de Windows Update

  Si esta opción está habilitada, se enviará información al Servidor de administración sobre las actualizaciones de Microsoft Windows Update que deban instalarse en los dispositivos cliente.

  Aunque deshabilite esta opción, ocasionalmente encontrará actualizaciones en la sección **Actualizaciones disponibles** de las propiedades de un dispositivo. Esto podría suceder, por ejemplo, cuando los dispositivos de la organización tengan vulnerabilidades que puedan repararse con esas actualizaciones.

  Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

  La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

- Detalles de las vulnerabilidades de software y las actualizaciones correspondientes

  Si esta opción está habilitada, se enviará información al Servidor de administración sobre las vulnerabilidades que se detecten en las aplicaciones de terceros instaladas en los dispositivos administrados (incluidas las aplicaciones de Microsoft) y sobre las actualizaciones disponibles para reparar vulnerabilidades en aplicaciones de terceros (excluidas, en este caso, las aplicaciones de Microsoft).

  Si habilita la opción **Detalles de las vulnerabilidades de software y las actualizaciones correspondientes**, aumentarán la carga en la red, la carga en el disco del Servidor de administración y el uso de recursos del Agente de red.

  Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

  Para administrar las actualizaciones de software de Microsoft, use la opción **Detalles de las actualizaciones de Windows Update**.

- **Detalles del Registro de hardware**

Actualizaciones y vulnerabilidades de software

En la sección **Actualizaciones y vulnerabilidades de software**, puede configurar la búsqueda de actualizaciones de Windows y habilitar la búsqueda de vulnerabilidades en los archivos ejecutables. La configuración en la sección **Actualizaciones y vulnerabilidades 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 **Conectarse al servidor de actualizaciones para actualizar los datos**.

Esta opción está seleccionada de forma predeterminada.

- **Pasivo**

  Si selecciona esta opción, el Agente de red se comunicará periódicamente con el Servidor de administración para enviarle información sobre las actualizaciones obtenidas durante la última sincronización entre el Agente de Windows Update y el origen de actualizaciones. Si el Agente de Windows Update no se sincroniza con un origen de actualizaciones, la información sobre actualizaciones del Servidor de administración se vuelve obsoleta.

  Seleccione esta opción si desea obtener actualizaciones de la caché del origen de actualizaciones.

- **Deshabilitado**

  Si selecciona esta opción, el Servidor de administración no solicitará información sobre las actualizaciones.

  Seleccione esta opción si, por ejemplo, desea probar primero las actualizaciones en su dispositivo local.

- **Analizar los archivos ejecutables en busca de vulnerabilidades al iniciarlos**

  Si habilita esta opción, cuando se inicie un archivo ejecutable, se lo analizará en busca de vulnerabilidades.

  Esta opción está deshabilitada de forma predeterminada.

Opciones de reinicio

En la sección **Opciones de reinicio**, puede indicar qué acción se llevará a cabo cuando se necesite reiniciar el sistema operativo de un dispositivo administrado para que una aplicación pueda instalarse, desinstalarse o utilizarse correctamente.

- **No reiniciar el sistema operativo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el sistema operativo automáticamente, 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 forma predeterminada.

  - Repetir la solicitud cada (min)

    Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

    Si no habilita esta opción, la solicitud se mostrará una sola vez.

  - Forzar reinicio después de (min)

    Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

    Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- Forzar el cierre de aplicaciones en sesiones bloqueadas

  Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

  Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

  Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

  Esta opción está deshabilitada de forma predeterminada.

Windows Desktop Sharing

En la sección **Windows Desktop Sharing**, puede 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 **Windows Desktop Sharing** están disponibles solo en dispositivos que ejecutan Windows:

- Habilitar auditoría

Habilite esta opción si desea auditar las operaciones que el administrador realice en el dispositivo remoto. Los registros de las acciones del administrador en el dispositivo remoto se computan:

- En el registro de eventos del dispositivo remoto
- en un archivo con la extensión syslog ubicado en la carpeta de instalación del Agente de red del dispositivo remoto
- en la base de datos de eventos de Kaspersky Security Center 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 forma predeterminada.

- **Máscaras de los archivos cuya lectura se debe supervisar**

  La lista contiene máscaras de archivos. Cuando la auditoría está habilitada, la aplicación monitorea los archivos de lectura del administrador que coinciden con las máscaras y guarda información sobre los archivos leídos. La lista está disponible si se ha marcado la casilla **Habilitar auditoría**. Puede editar máscaras de archivos y agregar máscaras nuevas a la lista. Cada máscara de archivo nueva se debe especificar en la lista en una línea nueva.

  De forma predeterminada, están especificadas las siguientes máscaras de archivos:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Máscaras de los archivos cuya modificación se debe supervisar**

  La lista contiene las máscaras de archivos en el dispositivo remoto. Cuando la auditoría está habilitada, la aplicación monitorea los cambios realizados por el administrador en los archivos que coinciden con las máscaras y guarda información sobre esas modificaciones. La lista está disponible si se ha marcado la casilla **Habilitar auditoría**. Puede editar máscaras de archivos y agregar máscaras nuevas a la lista. Cada máscara de archivo nueva se debe especificar en la lista en una línea nueva.

  De forma predeterminada, están especificadas las siguientes máscaras de archivos:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Administrar parches y actualizaciones

En la sección **Administrar parches y actualizaciones**, puede configurar la descarga y distribución de actualizaciones, así como la instalación de parches, en los dispositivos administrados. Habilite o deshabilite la opción **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes**.

Conectividad

La sección **Conectividad** incluye tres subsecciones:

- **Red**

- **Perfiles de conexión**
- **Programación de conexiones**

En la subsección **Red**, puede configurar la conexión al Servidor de administración, habilitar el uso de un puerto UDP y especificar el número de ese puerto UDP.

- En el grupo de opciones **Conexión con el Servidor de administración**, puede configurar los siguientes ajustes:
  - Comprimir tráfico de red

    Si esta opción está habilitada, se reducirá el volumen de datos transferido. En consecuencia, el Agente de red podrá transmitir información a mayor velocidad y el Servidor de administración deberá soportar menos carga.

    El uso de la CPU del equipo cliente podría aumentar.

    Esta casilla está activada de manera predeterminada.

  - Abrir puertos del Agente de red en el Firewall de Microsoft Windows

    Cuando se habilita esta opción, se agregan los puertos que el Agente de red necesita para funcionar a la lista de exclusiones del Firewall de Microsoft Windows.

    Esta opción está activada de forma predeterminada.

  - Utilizar la puerta de enlace de conexión del punto de distribución (si está disponible) con la configuración de conexión predeterminada

    Si esta opción está habilitada, la puerta de enlace de conexión del punto de distribución se usará con la configuración especificada en las propiedades del grupo de administración.

    Esta opción está activada de forma predeterminada.

- Usar puerto UDP

  Si necesita que el Agente de red se conecte al Servidor de administración a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un **número de puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado para conectarse al Servidor de administración es 15000.

- Número de puerto UDP

  En este campo, puede indicar el número del puerto UDP. El número de puerto predeterminado es 15000.

  El sistema decimal se usa para los registros.

  En dispositivos cliente con Windows XP Service Pack 2, el puerto UDP 15000 estará bloqueado por el firewall integrado. Deberá abrir el puerto manualmente.

- Utilizar el punto de distribución para forzar la conexión con el Servidor de administración

Seleccione esta opción si seleccionó 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 **Agregar** está inactivo. Tampoco se pueden modificar los perfiles de conexión preestablecidos.

En la subsección **Programación de conexiones**, puede especificar los intervalos de tiempo durante los cuales el Agente de red enviará datos al Servidor de administración:

- **Establecer conexión cuando sea necesario**
- **Establecer conexión en los intervalos que especifique**

En la subsección **Programación de conexiones**, puede especificar los intervalos de tiempo durante los cuales el Agente de red enviará datos al Servidor de administración:

- Establecer conexión cuando sea necesario

  Si se selecciona esta opción, la conexión se establece cuando el Agente de red debe enviar datos al Servidor de administración.

  Esta opción está seleccionada de forma predeterminada.

- Establecer conexión en los intervalos que especifique

  Si se selecciona esta opción, el Agente de red se conecta al Servidor de administración a una hora especificada. Puede agregar varios períodos de conexión.

Sondeo de red con puntos de distribución

En la sección **Sondeo de red con puntos de distribución**, puede configurar el sondeo automático de la red. 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 habilitada, el punto de distribución sondeará la red de manera automática, siguiendo la programación que se defina a través de los vínculos **Establecer programación de sondeo rápido** y **Establecer programación de sondeo completo**.

  Si se deshabilita esta opción, el Servidor de administración no sondeará la red.

  Esta opción está activada de forma predeterminada.

- Intervalos IP

Si esta opción está habilitada, el punto de distribución realizará sondeos de intervalos IP en forma automática, siguiendo la programación que se defina a través del vínculo **Establecer programación de sondeo**.

Si esta opción no está habilitada, el punto de distribución no hará sondeos de intervalos IP.

Esta opción está deshabilitada de forma predeterminada.

- Controladores de dominio

  Si se habilita esta opción, el punto de distribución sondeará automáticamente los controladores de dominio de acuerdo con la programación que configuró al hacer clic en el botón **Configurar programación de sondeos**.

  Si esta opción no está habilitada, el punto de distribución no hará sondeos de controladores de dominio.

  La frecuencia de sondeo de controladores de dominio para las versiones del Agente de red anteriores a la versión 10.2 se puede configurar en el campo **Intervalo de sondeo (min)**. El campo estará disponible si se habilita esta opción.

  Esta opción está deshabilitada de forma predeterminada.

Configuración de red para puntos de distribución

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 usar el servidor proxy para direcciones locales

  Si habilita esta opción, no se usará un servidor proxy para establecer conexión con los dispositivos de la red local.

  Esta opción está deshabilitada de forma predeterminada.

- Autenticación del servidor proxy

  Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

  Esta casilla no está marcada de manera predeterminada.

- **Nombre de usuario**
- **Contraseña**

Proxy de KSN (puntos de distribución)

En la sección **Proxy de KSN (puntos de distribución)**, puede configurar la aplicación para que utilice el punto de distribución para reenviar las solicitudes KSN desde los dispositivos administrados:

- **Habilitar el proxy de KSN en el lado del punto de distribución**

  El servicio de proxy de KSN se ejecuta en el dispositivo que se utiliza como punto de distribución. Utilice esta función para redistribuir y optimizar el tráfico de la red.

  Esta característica no estará disponible si el dispositivo que actúa como punto de distribución utiliza un sistema operativo 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 forma predeterminada. Esta opción solo se activa si la opción **Acepto utilizar 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 13111.

- **Puerto UDP**

  Si necesita que el Agente de red se conecte al Servidor de administración a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un **número de puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado para conectarse al Servidor de administración es 15000.

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	✓	✓	✓ Están disponibles las siguientes opciones:

		La opción **Detalles del Registro de hardware** está disponible.	• **Detalles de las aplicaciones instaladas** • **Detalles del Registro de hardware**
Actualizaciones y vulnerabilidades de software	✓	—	—
Opciones de reinicio	✓	—	—
Windows Desktop Sharing	✓	—	—
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 red con puntos de distribución	✓ Están disponibles las siguientes opciones: • **Red de Windows** • **Intervalos IP** • **Controladores de dominio** (Microsoft Active Directory)	—	✓ Están disponibles las siguientes opciones: • **Intervalos 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 avanzada contra amenazas**.

Para definir los ajustes recomendados para KSN:

1. En el menú principal, vaya a **Activos (dispositivos) → Directivas y perfiles**.
2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.
3. En las propiedades de la directiva, vaya a **Configuración de la aplicación → Protección avanzada contra amenazas → Kaspersky Security Network**.
4. Asegúrese de que la opción **Usar el 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. Habilite el uso de servidores KSN si el servicio del proxy de KSN no está disponible. Para ello, active la opción **Usar los servidores de Kaspersky Security Network cuando el servidor proxy de KSN no esté disponible**.

   Los servidores de KSN pueden estar alojados en la infraestructura de Kaspersky (este es el caso cuando se utiliza KSN) o en la infraestructura de un tercero (cuando se utiliza KPSN).
6. Haga clic en **Aceptar**.

Se guardan los ajustes recomendados para KSN.

Comprobar la lista de las redes protegidas por Firewall.

Asegúrese de que el Firewall de Kaspersky Endpoint Security para Windows proteja todas sus redes. De forma predeterminada, el Firewall protege las redes con los siguientes tipos de conexión:

- **Red pública**. Las aplicaciones de seguridad, los firewalls o los filtros no protegen los dispositivos de dicha red.
- **Red local**. El acceso a archivos e impresoras está restringido para dispositivos en esta red.
- **Red de confianza**. Los dispositivos en dicha red están protegidos contra ataques y accesos no autorizados a archivos y datos.

Si ha configurado una red personalizada, asegúrese de que el Firewall la proteja. Para ello, consulte la lista de redes en las propiedades de la directiva de Kaspersky Endpoint Security for Windows. La lista puede no contener todas las redes.

Para obtener más información acerca de Firewall, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

Para revisar la lista de redes:

1. En el menú principal, vaya a **Activos (dispositivos) → Directivas y perfiles**.

2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.

3. En las propiedades de la directiva, vaya a **Configuración de la aplicación → Protección básica contra amenazas → Firewall**.

4. En **Redes disponibles**, haga clic en el vínculo **Configuración de red**.

   Se abrirá la ventana **Conexiones de red**. La ventana contiene la lista de redes.

5. Si falta una red en la lista, agréguela.

Excluir detalles de software de la memoria del Servidor de administración

Recomendamos que el Servidor de administración no guarde información sobre los módulos de software que se inician en los dispositivos de red. De esta manera, se evita que se desborde la memoria del Servidor de administración.

Puede desactivar el almacenamiento de esta información en las propiedades de la directiva de Kaspersky Endpoint Security para Windows.

Para evitar que se guarde información sobre los módulos de software instalados:

1. En el menú principal, vaya a **Activos (dispositivos) → Directivas y perfiles**.

2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.

3. En las propiedades de la directiva, vaya a **Configuración de la aplicación → Configuración general → Informes y repositorios**.

4. En **Transferencia de datos al Servidor de administración**, si aún está activa en la directiva de nivel superior, desmarque la casilla **Acerca de las aplicaciones iniciadas**.

   Cuando esta casilla está seleccionada, la base de datos del Servidor de administración guarda la información acerca de todas las versiones de todos los módulos de software en los dispositivos en red. Esta información puede ocupar una gran cantidad de espacio 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

Recomendamos guardar únicamente eventos que sean de importancia en la base de datos del Servidor de administración; ello ayudará a no sobrepasar la capacidad de esta base de datos. Para los eventos que considere poco importantes, puede reducir o deshabilitar 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 **Guardar en la base de datos del Servidor de administración por (días)** está activada y, a continuación, ingrese 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 **Guardar en la base de datos del Servidor de administración por (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 **Al descargar nuevas actualizaciones al repositorio** cuando la casilla de verificación **Utilizar retardo aleatorio automático para el inicio de la tarea** está seleccionada.

Tareas

En esta sección se describen las tareas utilizadas por Kaspersky Security Center Cloud Console.

Acerca de las tareas

Para administrar las aplicaciones de seguridad de Kaspersky instaladas en los dispositivos a través de Kaspersky Security Center Cloud Console, es necesario crear y ejecutar tareas. Las *tareas* son el medio que se utiliza para instalar, iniciar y detener aplicaciones, analizar archivos, actualizar bases de datos y módulos de software y realizar otras acciones en las aplicaciones. 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 dos personas: el administrador (a través de sus herramientas administrativas) y el usuario del dispositivo remoto (mediante, por ejemplo, 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 múltiples tareas de grupo, tareas globales o tareas locales.

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

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

Los resultados de ejecución de las tareas se guardan en el registro de eventos del sistema operativo en cada dispositivo 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 seleccionar dispositivos en la lista **Dispositivos administrados** y luego crear una nueva tarea asignada a los dispositivos seleccionados.

Para crear una tarea en la lista de tareas:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga las instrucciones.
3. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.
4. Haga clic en el botón **Finalizar**.

Se crea la tarea y se la agrega a la lista de tareas.

Para crear una nueva tarea asignada a los dispositivos seleccionados:

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 han creado 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 de forma remota* está relacionada con el Servidor de administración y *Buscar vulnerabilidades y actualizaciones requeridas* se refiere al Agente de red.

Para ver las propiedades de una tarea:

Haga clic en el nombre de la tarea.

Aparece la ventana de propiedades de la tarea. En ella encontrará una serie de pestañas con nombre. La pestaña llamada **General** contiene la propiedad **Tipo de tarea**, por ejemplo, y si ingresa a la pestaña **Programación**, encontrará la programación de la tarea.

Iniciar una tarea manualmente

La aplicación inicia las tareas siguiendo la programación configurada en las propiedades de cada tarea. Puede iniciar una tarea de forma manual en cualquier momento desde la lista de tareas. Como alternativa, puede seleccionar dispositivos en la lista **Dispositivos administrados** y, luego, iniciar una tarea existente para ellos.

Para iniciar una tarea manualmente:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. En la lista de tareas, marque la casilla ubicada junto a la tarea que desee iniciar.
3. Haga clic en el botón **Iniciar**.

Se inicia la tarea. Puede verificar el estado de la tarea en la columna **Estado** o haciendo clic en el botón **Resultado**.

Iniciar una tarea para dispositivos puntuales

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 seleccionados al ejecutar la tarea.

Para iniciar una tarea para dispositivos puntuales:

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 los dispositivos para los que desee ejecutar la tarea. Puede utilizar las funciones de búsqueda y filtrado para encontrar los dispositivos de su interés.

2. Haga clic en el botón **Ejecutar tarea** y, luego, seleccione **Aplicar tarea existente**.

   Se muestra la lista de 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 ubicado sobre la lista para buscar la tarea por nombre. Solo se puede seleccionar una única 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 modifica.

Ajustes 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 la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

  - Especificar las direcciones de los dispositivos manualmente o importarlas de una lista

La tarea se asignará a ciertos dispositivos específicos. Para seleccionar los dispositivos, puede usar alguno de estos métodos:

- Indicar la dirección IP, el nombre NetBIOS o el nombre DNS del dispositivo.
- Indicar un intervalo de direcciones IP.

  Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.
- Seleccionar los dispositivos detectados por el Servidor de administración, incluso si aún no están en un grupo de administración.

  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 ser útil para, por ejemplo, ejecutar una tarea en los 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 forma predeterminada.

  - **Especificar cuenta**

    Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

- 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 mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

  - **Reiniciar el dispositivo**

Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

  Si no habilita esta opción, la solicitud se mostrará una sola vez.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

  Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

  Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

  Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

  Esta opción está deshabilitada de forma predeterminada.

Ajustes que se configuran tras crear una tarea

Los siguientes ajustes pueden definirse solamente cuando la tarea ya se ha creado.

- Ajustes para tareas de grupo:

- Distribuir a subgrupos

  Esta opción solo está disponible en los ajustes de tareas de grupo.

  Cuando esta opción está habilitada, el alcance de la tarea incluye lo siguiente:

  - El grupo de administración que se seleccionó al crear la tarea.
  - Los grupos de administración subordinados al grupo de administración seleccionado y ubicados en cualquier nivel de la jerarquía de grupos.

  Cuando esta opción está deshabilitada, el alcance de la tarea incluye solo el grupo de administración que se seleccionó al crear la tarea.

  Esta opción está activada de forma predeterminada.

- Distribuir a Servidores de administración secundarios y virtuales

  Cuando esta opción está habilitada, la tarea aplicada al Servidor de administración principal se aplica también a los servidores de administración secundarios (incluidos los virtuales). Si ya existe una tarea del mismo tipo en un Servidor de administración secundario, se aplican ambas tareas a ese servidor (la existente y la heredada del Servidor de administración principal).

  Esta opción solo está disponible cuando la opción **Distribuir a subgrupos** está habilitada.

  Esta opción está deshabilitada de forma predeterminada.

- Programación de la tarea:
  - **Iniciar tarea (ajuste):**
    - Manual

      La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

      Esta opción está seleccionada de forma predeterminada.

    - Una vez

      La tarea se ejecuta una vez, en la fecha y hora especificadas (de manera predeterminada, el día en que se creó la tarea).

    - Inmediatamente

      La tarea se ejecuta inmediatamente después de guardar su configuración.

    - Cada N minutos

      La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

      De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

    - Cada N horas

La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

- **Cada N días**

  La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

  De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

- **Por días de la semana**

  La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

  De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00 p. m.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  De manera predeterminada, no se selecciona ningún día del mes. La hora de inicio predeterminada es a las 18:00.

- **Al descargar nuevas actualizaciones al repositorio**

  Cuando se descarguen nuevas actualizaciones en los repositorios de los puntos de distribución, Kaspersky Security Center Cloud Console ejecutará todas las tareas que tengan esta programación. El Agente de red verifica si hay actualizaciones disponibles cada vez que el dispositivo administrado se sincroniza con el Servidor de administración (la sincronización se lleva a cabo con una periodicidad denominada "latido").

  Esta programación podría resultar útil para, por ejemplo, la tarea "Actualizar" de Kaspersky Endpoint Security o de otra aplicación de seguridad.

  Si el Agente de red de un dispositivo administrado no detecta actualizaciones nuevas durante 25 horas o más, Kaspersky Security Center Cloud Console ejecutará en ese dispositivo todas las tareas que tengan esta programación. Las tareas volverán a ejecutarse cada una hora hasta que se detecten nuevas actualizaciones. Kaspersky Security Center Cloud Console también ejecutará estas tareas cada una hora si no hay conexión entre el dispositivo administrado y el punto de distribución que descarga las actualizaciones al repositorio.

- **Ante brotes de virus**

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completarse otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. 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 el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

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
Mensual	Sí
Cada mes en los días especificados de semanas seleccionadas	Sí
Al descargar nuevas actualizaciones al repositorio	Otro disparador para ejecutar la tarea (corresponde al nombre del programa)
Ante brotes de virus	Otro disparador para ejecutar la tarea (corresponde al nombre del programa)
Al completarse 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)
Manual	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 **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- **Utilizar retardo aleatorio automático para el inicio de la tarea**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- Utilizar el retardo aleatorio automático para el inicio de la tarea dentro de un intervalo de

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

- Encender dispositivos mediante la función Wake-on-LAN antes de iniciar la tarea

  El sistema operativo del dispositivo se iniciará a la hora especificada antes de que se ejecute la tarea. El período de tiempo predeterminado es de cinco minutos.

  Habilite esta opción si desea que la tarea se ejecute en todos los dispositivos cliente que formen parte del alcance de la tarea, incluidos aquellos que se encuentren apagados cuando la tarea esté próxima a comenzar.

  Si desea que el dispositivo se apague automáticamente una vez completada la tarea, habilite la opción **Apagar dispositivos cuando se complete la tarea**. Encontrará esta opción en la misma ventana.

  Esta opción está deshabilitada de forma predeterminada.

- Apagar los dispositivos después de completar la tarea

  Esta opción puede ser útil para, por ejemplo, una tarea que actualice los dispositivos cliente todos los viernes después del horario laboral y luego los apague para que no consuman energía el fin de semana.

  Esta opción está deshabilitada de forma predeterminada.

- Detener la tarea si tarda más de

  Una vez que transcurra el período especificado, la tarea se detendrá automáticamente, se haya completado o no.

  Habilite esta opción si desea que las tareas que tarden mucho en completarse se interrumpan o se detengan.

  Esta opción está deshabilitada de forma predeterminada. El tiempo de ejecución por defecto para las tareas es de 120 minutos.

- Notificaciones:

  - Bloque **Almacenar el historial de la tarea**:

    - **Guardar todos los eventos**
    - **Guardar eventos relacionados con el progreso de la tarea**
    - **Guardar solo los resultados de la ejecución de la tarea**
    - Guardar en la base de datos del Servidor de administración por (días)

El Servidor de administración conservará por el número de días especificado los eventos de la aplicación que estén relacionados con la ejecución de la tarea en los dispositivos cliente incluidos en el alcance de la tarea. Transcurrido este período, la información se eliminará del Servidor de administración.

Esta opción está activada de forma predeterminada.

- Guardar en el registro de eventos del SO del dispositivo

  Los eventos de la aplicación relacionados con la ejecución de la tarea se almacenarán localmente en el registro de eventos de Windows de cada dispositivo cliente.

  Esta opción está deshabilitada de forma predeterminada.

- **Notificar solo acerca de los errores**
- **Notificar por correo electrónico**

- Ajustes del alcance de la tarea
- Exclusiones del alcance

  Podrá definir grupos de dispositivos a los que no se aplicará la tarea. Los grupos excluidos solo pueden ser subgrupos del grupo de administración al que se aplica la tarea.

- **Historial de revisiones**

Exportar una tarea

Kaspersky Security Center Cloud Console permite guardar una tarea y su configuración en un archivo KLT. El archivo KLT puede usarse para importar la tarea guardada en Kaspersky Security Center Windows o Kaspersky Security Center Linux.

Para exportar una tarea:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Marque la casilla ubicada junto a la tarea que desee exportar.

   No es posible exportar más de una tarea a la vez. Si selecciona más de una tarea, el botón **Exportar** se desactivará. Las tareas del Servidor de administración tampoco pueden exportarse.
3. Haga clic en el botón **Exportar**.
4. En la ventana **Guardar como** que se abrirá, ingrese la ruta y el nombre del archivo en que se guardará la tarea. Haga clic en el botón **Guardar**.

   La ventana **Guardar como** aparecerá solo si utiliza los navegadores Google Chrome, Microsoft Edge u Opera. Si utiliza otro navegador, el archivo de la tarea se guardará automáticamente en la carpeta **Descargas**.

Importar una tarea

Kaspersky Security Center Cloud Console permite importar una tarea guardada en un archivo KLT. El archivo KLT contiene la tarea exportada y su configuración.

Para importar una tarea:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en el botón **Importar**.
3. Haga clic en el botón **Examinar** para elegir el archivo de tareas que desee importar.
4. En la ventana que se abrirá, ingrese la ruta al archivo KLT de la tarea y haga clic en el botón **Abrir**. Tenga en cuenta que no podrá seleccionar más de un archivo de tarea.

   Comenzará a procesarse la tarea.
5. Una vez que la tarea se haya procesado, seleccione los dispositivos a los que desee asignarla. Para ello, seleccione una de las siguientes opciones:

   - **Asignar tarea a un grupo de administración**

     La tarea se asignará a los dispositivos incluidos en un grupo de administración. Puede seleccionar un grupo existente o crear uno nuevo.

     Puede usar esta opción para, por ejemplo, ejecutar una tarea que envíe un mensaje a ciertos usuarios si el contenido atañe solamente a los dispositivos de un grupo de administración puntual.

     Si la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

   - **Especificar las direcciones de los dispositivos manualmente o importarlas de una lista**

     Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

     Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

   - **Asignar tarea a una selección de dispositivos**

     La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

     Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.
6. Elija el alcance de la tarea.
7. Haga clic en el botón **Completado** para finalizar la importación de la tarea.

Aparecerá una notificación con los resultados de la importación. Si la tarea se importa correctamente, puede hacer clic en el vínculo **Detalles** para ver las propiedades de la misma.

Una vez que se complete la importación, la tarea aparecerá en la lista de tareas. También se importarán la configuración y la programación de la tarea. La tarea se iniciará de acuerdo con su programación.

Si la tarea importada tiene el mismo nombre que una tarea existente, el nombre de la tarea importada se complementará con un índice secuencial en formato **(<siguiente número secuencial>)**, por ejemplo **(1)** o **(2)**.

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 vínculo **Resultados** para abrir la ventana **Resultados de la 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 puede incluirse en un solo grupo de administración. Los dispositivos se pueden asignar a un grupo automáticamente según las **Condiciones de la regla:**

- Crear reglas de movimiento de dispositivos.
- Copiar reglas de movimiento de dispositivos.
- Condiciones para una regla de movimiento de dispositivos.

Puede usar selecciones de dispositivos para filtrar dispositivos según una condición. También puede etiquetar dispositivos para crear selecciones, para buscar dispositivos y para distribuir dispositivos entre grupos de administración.

Configuración de un dispositivo administrado

Para ver la configuración de un dispositivo administrado:

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

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo de su interés.

Se muestra la ventana de propiedades del dispositivo seleccionado.

Las siguientes pestañas se muestran en la parte superior de la ventana de propiedades y representan los principales grupos de ajustes:

- General

Esta pestaña incluye las siguientes secciones:

- La sección **General** muestra información general sobre el dispositivo cliente. La información se basa en los datos recibidos durante la última sincronización del dispositivo cliente con el Servidor de administración.

  - **Nombre**

    En este campo, puede ver y modificar el nombre asignado al dispositivo cliente en el grupo de administración.

  - **Descripción**

    En este campo, puede ingresar una descripción adicional para el dispositivo cliente.

  - **Estado del dispositivo**

    Estado del dispositivo cliente, asignado sobre la base de los criterios definidos por el administrador para el estado de protección antivirus del dispositivo y la actividad del dispositivo en la red.

  - **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 completo del grupo**

    Grupo de administración en el que está incluido el dispositivo cliente.

  - **Última actualización de las bases de datos antivirus**

    Fecha en que las bases de datos o las aplicaciones del antivirus se actualizaron por última vez en el dispositivo.

  - **Conectado al Servidor de administración**

    Fecha y hora en que el Agente de red instalado en el dispositivo cliente se conectó al Servidor de administración por última vez.

  - **Visible por última vez**

    Fecha y hora en que el dispositivo se vio en la red por última vez.

  - **Versión del Agente de red**

    Versión del Agente de red instalado.

- **Creado**

  Fecha de creación del dispositivo en Kaspersky Security Center 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 una tabla con información sobre los usuarios que están conectados al dispositivo actualmente. La tabla muestra los siguientes datos en las columnas correspondientes:

  - Nombre de usuario
  - Nombre de cuenta 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 la 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 protección**

Este campo muestra el estado de la protección en tiempo real del dispositivo cliente.

Si el estado se modifica en el dispositivo, el cambio no se verá reflejado en la ventana de propiedades del dispositivo sino hasta que el dispositivo se sincronice con el Servidor de administración.

- Último análisis completo

  Fecha y hora del último análisis antimalware realizado en el dispositivo cliente.

- Virus detectados

  Cantidad total de amenazas detectadas en el dispositivo cliente desde la instalación de la aplicación de seguridad (primer análisis) o desde la última vez que el contador de amenazas se puso en cero.

- Objetos que no se pudieron desinfectar

  Número de archivos no procesados en el dispositivo cliente.

  Este campo no refleja el número de archivos no procesados en dispositivos móviles.

- Estado de cifrado del disco

  Estado del cifrado de archivos en las unidades locales del dispositivo. Para obtener una descripción de los estados, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

- La sección **Estado del dispositivo definido por la aplicación** proporciona información sobre el estado del dispositivo definido por la aplicación administrada instalada en el dispositivo. Este estado puede no coincidir con el 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.

- Directivas y perfiles de directivas activos

  Esta pestaña enumera las directivas y los perfiles de directivas que están asignados al dispositivo administrado en un momento dado.

- Tareas

La pestaña **Tareas** permite administrar las tareas del dispositivo cliente. Utilice esta sección para crear tareas nuevas, ver la lista de tareas existentes, ver los resultados de ejecución de las tareas e iniciar, detener, eliminar y reconfigurar las tareas existentes. La lista de tareas mostrada se basa en los datos recibidos durante la última sesión de sincronización entre el cliente y el Servidor de administración. El Servidor de administración solicita detalles sobre el estado de las tareas al dispositivo cliente. Si el puerto 15000 UDP está disponible en el dispositivo administrado para recibir notificaciones push del Servidor de administración, se muestra el estado de la tarea y se activan los botones para administrar la tarea. Si el dispositivo administrado no está disponible para notificaciones push, pero el modo de conexión continua al Servidor de administración está activado (la opción **No desconectar del Servidor de administración** en la sección **General** está activada), las acciones con tareas también están disponibles.

Si no se establece una conexión, no se muestra el estado y los botones quedan desactivados.

- **Eventos**

  La pestaña **Eventos** muestra los eventos registrados en el Servidor de administración para el dispositivo cliente seleccionado.

- **Problemas de seguridad**

  En la pestaña **Problemas de seguridad**, puede ver, crear y editar problemas de seguridad para el dispositivo cliente. Los problemas de seguridad se pueden crear manualmente por el administrador o automáticamente por las aplicaciones de Kaspersky administradas que se han instalado en el dispositivo cliente. El administrador podría crear un problema de seguridad si, por ejemplo, algunos de sus usuarios han copiado malware de una unidad extraíble en más de una ocasión. En el texto del problema de seguridad, el administrador podría brindar una breve descripción del caso, delinear las acciones que recomienda tomar (por ejemplo, medidas disciplinarias contra los usuarios) y agregar un vínculo al usuario o a los usuarios.

  Se denomina *procesado* al problema de seguridad para el cual se han tomado todas las medidas necesarias. La presencia de problemas de seguridad no procesados puede usarse como condición para cambiar el estado de un dispositivo a *Crítico* o *Advertencia*.

  En esta sección, encontrará una lista con problemas de seguridad que se hayan creado para el dispositivo. Los problemas de seguridad se clasifican por tipo y por nivel de gravedad. El tipo de problema de seguridad lo define la aplicación de Kaspersky que crea el problema de seguridad. Si desea resaltar los problemas de seguridad procesados de la lista, marque la casilla de la columna **Procesado**.

- **Etiquetas**

  La pestaña **Etiquetas** permite administrar la lista de palabras clave que se utilizan para buscar dispositivos cliente. Aquí puede ver la lista de etiquetas existentes, asignar etiquetas incluidas en la lista, configurar reglas de etiquetado automático, agregar etiquetas nuevas, eliminar etiquetas antiguas y modificar el nombre de las etiquetas existentes.

- **Avanzado**

Esta pestaña incluye las siguientes secciones:

- **Registro de aplicaciones**. En esta sección, puede ver un registro de las aplicaciones instaladas en el dispositivo cliente y de las actualizaciones de esas aplicaciones; también puede configurar el modo de visualización del registro de aplicaciones.

  Podrá ver información sobre las aplicaciones instaladas si el Agente de red instalado en el dispositivo cliente le envía la información necesaria al Servidor de administración. Puede configurar el envío de información al Servidor de administración en la ventana de propiedades del Agente de red o en su directiva, en la sección **Repositorios**.

  Al hacer clic en el nombre de una aplicación, se abre una ventana que contiene los detalles de la aplicación y una lista de los paquetes de actualización instalados para la aplicación.

- **Archivos ejecutables**. Esta sección muestra los archivos ejecutables almacenados en el dispositivo cliente.

- **Puntos de distribución**. Esta sección contiene una lista de los puntos de distribución con los que interactúa el dispositivo.

  - Exportar a archivo

    Haga clic en el botón **Exportar a archivo** para guardar en un archivo la lista de puntos de distribución con los que interactúa el dispositivo. De manera predeterminada, la aplicación exporta la lista de dispositivos a un archivo CSV.

  - Propiedades

    Haga clic en el botón **Propiedades** para ver y configurar el punto de distribución con el que interactúa el dispositivo.

- **Registro de hardware**. En esta sección, puede ver información sobre el hardware instalado en el dispositivo cliente.

  Si el Agente de red está instalado en un dispositivo con Windows, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo:

  - RAM
  - Dispositivos de almacenamiento
  - Placa madre
  - CPU
  - Adaptadores de red
  - Monitores
  - Adaptador de video
  - Tarjeta de sonido

  Si el Agente de red está instalado en un dispositivo con Linux o macOS, envía al Servidor de administración la siguiente información sobre el hardware del dispositivo, si el sistema operativo la proporciona:

- Volumen total de la RAM
- Volumen total de los dispositivos de almacenamiento masivo
- Placa madre
- CPU
- Adaptadores de red

- **Actualizaciones disponibles**. Esta sección muestra las actualizaciones de software que se han encontrado en el dispositivo, pero que aún no se han instalado.

- **Vulnerabilidades de software**. Esta sección muestra información sobre las vulnerabilidades de las aplicaciones de terceros instaladas en los dispositivos cliente.

  Para guardar las vulnerabilidades en un archivo, marque las casillas ubicadas junto a las vulnerabilidades que desea guardar, y luego haga clic en el botón **Exportar a CSV** o en el botón **Exportar a TXT**.

  La sección contiene los siguientes ajustes:

  - Mostrar solo las vulnerabilidades que pueden repararse

    Si habilita esta opción, la sección mostrará las vulnerabilidades que se puedan reparar con un parche.

    Si deshabilita esta opción, la sección mostrará tanto las vulnerabilidades que se puedan reparar con un parche como las vulnerabilidades para las que no exista parche publicado.

    Esta opción está activada de forma predeterminada.

  - Prop. de la vulnerabilidad

    Haga clic en el nombre de una vulnerabilidad de software de la lista para ver las propiedades de la vulnerabilidad de software seleccionada en una ventana aparte. En la ventana, puede hacer lo siguiente:

    - Hacer que la vulnerabilidad de software se ignore en el dispositivo administrado (en la Consola de administración o en Kaspersky Security Center Cloud Console).
    - Ver la lista de reparaciones recomendadas para la vulnerabilidad.
    - Designar manualmente las actualizaciones de software con las que se reparará 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.

- **Diagnóstico remoto**. 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 estado Crítico**, **Protección deshabilitada**, **Se han detectado amenazas activas**). Las selecciones predefinidas no se pueden eliminar. De ser necesario, puede crear y configurar selecciones adicionales, llamadas *selecciones definidas por el usuario*.

En una selección definida por el usuario, se puede determinar el alcance de la búsqueda y seleccionar todos los dispositivos, los dispositivos administrados o los dispositivos no asignados. Los parámetros de búsqueda se especifican en las condiciones. Una selección de dispositivos puede tener varias condiciones con diferentes parámetros de búsqueda. Puede, por ejemplo, crear dos condiciones y especificar intervalos IP diferentes en cada una de ellas. Una selección con varias condiciones muestra los dispositivos que cumplen con cualquiera de esas condiciones. Por el contrario, los parámetros de búsqueda especificados en una condición se superponen. Si una condición especifica tanto un intervalo IP como el nombre de una aplicación instalada, se mostrarán únicamente los dispositivos que tengan asignada una dirección IP de ese intervalo y que tengan instalada esa aplicación.

Ver la lista de dispositivos de una selección de dispositivos

Kaspersky Security Center Cloud Console le permite ver la lista de dispositivos desde una selección de dispositivos.

Para ver la lista de dispositivos de una selección de dispositivos:

1. En el menú principal, vaya a las secciones **Activos (dispositivos)** → **Selecciones de dispositivos** o **Descubrimiento y despliegue** → **Selecciones de dispositivos**.
2. En la lista de selecciones, haga clic en el nombre de la selección de dispositivos.

   La página muestra una tabla con información sobre los dispositivos incluidos en la selección de dispositivos.
3. Puede hacer lo siguiente para agrupar y filtrar los datos que conforman la tabla de dispositivos:

   - Haga clic en el ícono de configuración (⚙) y seleccione las columnas que se deban mostrar en la tabla.
   - Haga clic en el ícono de filtro (▽) y, en el menú que se abrirá, defina el criterio de filtrado.

     Se mostrará la tabla de dispositivos filtrada.

Puede seleccionar uno o varios dispositivos en la selección de dispositivos y hacer clic en el botón **Nueva tarea** para crear una tarea que se aplicará a estos dispositivos.

Para mover los dispositivos seleccionados de la selección de dispositivos a otro grupo de administración, haga clic en el botón **Mover a un grupo** y luego seleccione el grupo de administración de destino.

Crear una selección de dispositivos

Para crear una selección de dispositivos:

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

   Se muestra una página con una lista de selecciones de dispositivos.
2. Haga clic en el botón **Agregar**.

Se abre la ventana **Configuración de la selección de dispositivos**.

3. Escriba el nombre de la nueva selección.
4. Especifique el grupo que contiene los dispositivos que desea incluir en la selección de dispositivos:

   - **Buscar cualquier dispositivo**: Buscar dispositivos que cumplan con los criterios de selección y que estén incluidos en el grupo **Dispositivos administrados** o **Dispositivos no asignados**.
   - **Buscar dispositivos administrados**: Buscar dispositivos que cumplan con los criterios de selección y que estén incluidos en el grupo **Dispositivos administrados**.
   - **Buscar dispositivos no asignados**: Buscar dispositivos que cumplan con los criterios de selección y que estén incluidos en el grupo **Dispositivos no asignados**.

   Puede habilitar la casilla de verificación **Incluir datos de Servidores de administración secundarios** para habilitar la búsqueda de dispositivos que cumplan con los criterios de selección y que estén administrados por Servidores de administración secundarios.

5. Haga clic en el botón **Agregar**.
6. En la ventana que se abre, especifique las condiciones que deben cumplirse para incluir los dispositivos en esta selección y, a continuación, haga clic en el botón **Aceptar**.
7. Haga clic en el botón **Guardar**.

La selección de dispositivos se crea y se agrega a la lista de selecciones de dispositivos.

Configurar una selección de dispositivos

Para configurar una selección de dispositivos:

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

   Se muestra una página con una lista de selecciones de dispositivos.

2. Elija la selección de dispositivos definida por el usuario pertinente y haga clic en el botón **Propiedades**.

   Se abre la ventana **Configuración de la selección de dispositivos**.

3. En la pestaña **General**, haga clic en el vínculo **Nueva condición**.
4. Especifique las condiciones que deban cumplirse para que un dispositivo se incluya o no en la selección.
5. Haga clic en el botón **Guardar**.

El cambio se aplica y se guarda.

A continuación, se presentan descripciones de las condiciones para asignar dispositivos a una selección. Las condiciones se combinan usando el operador lógico OR: la selección incluirá dispositivos que cumplan con, al menos, una de las condiciones de la lista.

General

En la sección **General**, puede cambiar el nombre de una condición de la selección y especificar si esa condición se debería invertir:

Invertir condición de selección

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 forma 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.

- Intervalo IP

  Si habilita esta opción, podrá ingresar las direcciones IP inicial y final del intervalo IP en el que deberán estar incluidos los dispositivos pertinentes.

  Esta opción está deshabilitada de forma predeterminada.

- Administrado por un Servidor de administración diferente

Seleccione uno de los siguientes valores:

- **Sí**. Una regla de movimiento de dispositivos solo se aplica a los dispositivos cliente administrados por otros Servidores de administración. Estos servidores son diferentes del servidor en el que configura la regla de movimiento de dispositivos.
- **No**. La regla de movimiento de dispositivos solo se aplica a los dispositivos cliente administrados por el Servidor de administración actual.
- **Ningún valor seleccionado**. La condición no se aplica.

En la sección **Active Directory**, puede configurar criterios para dispositivos incluidos en una selección según sus datos de Active Directory:

- El dispositivo está en una unidad organizativa de Active Directory

  Si habilita esta opción, la selección incluirá los dispositivos de la unidad organizativa de Active Directory especificada en el campo de entrada.

  Esta opción está deshabilitada de forma predeterminada.

- Incluir unidades 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 forma predeterminada.

- El dispositivo es miembro de un grupo de Active Directory

  Si habilita esta opción, la selección incluirá los dispositivos que pertenezcan al grupo de Active Directory especificado en el campo de entrada.

  Esta opción está deshabilitada de forma predeterminada.

En la sección **Actividad de red**, puede establecer los criterios que se usarán para incluir dispositivos en la selección basándose en la actividad de red de los mismos:

- Actúa como punto de distribución

  En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

  - **Sí**. La selección incluirá dispositivos que funcionen como punto de distribución.
  - **No**. La selección no incluirá dispositivos que funcionen como punto de distribución.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- No desconectar del Servidor de administración

En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

- **Habilitado**. La selección incluirá dispositivos en los que esté activada la casilla **No desconectar del Servidor de administración**.
- **Deshabilitado**. La selección incluirá dispositivos en los que no esté activada la casilla **No desconectar del Servidor de administración**.
- **Ningún valor seleccionado**. El criterio no se aplicará.

- Perfil de conexión cambiado

En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

- **Sí**. La selección incluirá dispositivos que se hayan conectado al Servidor de administración tras un cambio de perfil de conexión.
- **No**. La selección no incluirá dispositivos que se hayan conectado al Servidor de administración tras un cambio de perfil de conexión.
- **Ningún valor seleccionado**. El criterio no se aplicará.

- Última conexión con el Servidor de administración

Puede utilizar esta casilla para establecer un criterio de búsqueda de dispositivos que se base en el momento en el que haya ocurrido la última conexión al Servidor de administración.

Si activa esta casilla, podrá usar los campos de entrada para indicar el intervalo de tiempo (fecha y hora) en el que deberá haber ocurrido la última conexión entre el Agente de red instalado en el dispositivo cliente y el Servidor de administración. La selección incluirá aquellos dispositivos que estén alcanzados por el intervalo especificado.

Si no activa esta casilla, no se aplicará este criterio.

Esta casilla no está marcada de manera predeterminada.

- Nuevos dispositivos detectados por sondeo de red

Utilice esta opción para buscar dispositivos nuevos, que se hayan detectado durante los sondeos de red realizados en días recientes.

Si habilita esta opción, la selección incluirá solo aquellos dispositivos nuevos que se hayan detectado mediante el descubrimiento de dispositivos en el intervalo de días especificado en el campo **Periodo de detección (días)**.

Si deshabilita esta opción, la selección incluirá todos los dispositivos detectados por el mecanismo de descubrimiento.

Esta opción está deshabilitada de forma predeterminada.

- Dispositivo visible

En la lista desplegable, puede establecer el criterio que se usará para incluir dispositivos en la selección cuando se realice la búsqueda:

- **Sí**. La selección incluirá aquellos dispositivos que sean visibles en la red.
- **No**. La selección incluirá aquellos dispositivos que no sean visibles en la red.
- **Ningún valor seleccionado**. El criterio no se aplicará.

En la sección **Segmentos de nube**, puede configurar criterios para incluir dispositivos en una selección según sus respectivos segmentos de nube:

- El dispositivo se encuentra en un segmento de la nube

  Si esta opción está habilitada, puede elegir dispositivos de los segmentos de nube de AWS, Azure y Google.

  Si también habilita la opción **Incluir objetos secundarios**, la búsqueda se realizará en todos los objetos secundarios del segmento elegido.

  Los resultados de la búsqueda solo incluirán aquellos dispositivos que estén en el segmento seleccionado.

- Dispositivo encontrado mediante API

  La lista desplegable le permite operar con el hecho de que el dispositivo pueda detectarse con las herramientas provistas por una API.

  - **Sí**. El dispositivo se detecta mediante el uso de la API de AWS, Azure o Google.
  - **No**. El dispositivo no se puede detectar mediante el uso de la API de AWS, Azure o Google. Es decir, o bien el dispositivo no se encuentra en el entorno de nube, o bien sí está en el entorno de nube, pero, por algún motivo, no se lo puede detectar con una API.
  - Ningún valor. Esta condición no se aplica.

Estados de los dispositivos

En la sección **Estado del dispositivo administrado**, puede configurar criterios para incluir dispositivos en una selección según la descripción del estado de dispositivos desde una aplicación administrada:

- Estado del dispositivo

  Lista desplegable en la que puede seleccionar un estado de dispositivo: *Sin inconvenientes*, *Crítico* o *Advertencia*.

- Estado de protección en tiempo real

  Lista desplegable en la cual puede seleccionar el estado de la protección en tiempo real. La selección incluirá aquellos dispositivos que tengan el estado de protección en tiempo real indicado.

- Descripción del estado del dispositivo

En este campo, puede activar casillas correspondientes a condiciones que, al cumplirse, hacen que el dispositivo tome uno de los siguientes estados: *Sin inconvenientes, Crítico* o *Advertencia*.

En la sección **Estado de componentes en aplicaciones administradas**, puede configurar los criterios para incluir dispositivos en una selección según los estados de los componentes de las aplicaciones administradas:

- Estado de Prevención de fugas de datos

  Buscar dispositivos basándose en el estado de Prevención de fuga de datos (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error*).

- Estado de protección de los servidores de colaboración

  Buscar dispositivos basándose en el estado de la protección para servidores de colaboración (*Desconocido*, *Detenida*, *Iniciándose, En pausa*, *En ejecución*, *Error*).

- Estado de protección antivirus en servidores de correo

  Buscar dispositivos basándose en el estado de la protección para servidores de correo (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error).*

- Estado de Sensor de Endpoint

  Buscar dispositivos basándose en el estado del componente Sensor de Endpoint (*Desconocido, Detenida, Iniciándose, En pausa, En ejecución, Error*).

En la sección **Problemas que afectan al estado en las aplicaciones administradas**, puede especificar los criterios que se utilizarán para incluir dispositivos en la selección de acuerdo con la lista de posibles problemas detectados por una aplicación administrada. Si un dispositivo tiene al menos uno de los problemas elegidos, ese dispositivo se incluirá en la selección. Cuando selecciona un problema listado para varias aplicaciones, tiene la opción de seleccionar este problema en todas las listas automáticamente.

Puede activar casillas correspondientes a las descripciones de estado reportadas por la aplicación administrada. Cuando se reciban esos estados, los dispositivos correspondientes se incluirán en la selección. Si elige un estado incluido en las listas de varias aplicaciones, tendrá la opción de seleccionar todos los casos automáticamente.

Datos del sistema

En la sección **Sistema operativo**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según el tipo de sistema operativo.

- Tipo de plataforma

  Si activa esta casilla, podrá seleccionar un sistema operativo de la lista. Los dispositivos que tengan instalado ese sistema operativo se incluirán en los resultados de búsqueda.

- Versión del Service Pack del sistema operativo

En este campo, puede especificar la versión del paquete de su sistema operativo (en formato *X.Y.*), que determinará cómo aplicar la regla de migración a su dispositivo. De manera predeterminada, no hay una versión definida.

- Arquitectura del sistema operativo

  En la lista desplegable, puede seleccionar la arquitectura para la que deberá estar diseñado el sistema operativo. Los valores posibles son **Desconocido**, **x86**, **AMD64** e **IA64**. La arquitectura que elija determinará el modo de aplicar la regla de movimiento al dispositivo. De manera predeterminada, no hay ninguna opción seleccionada en la lista (es decir, la arquitectura del sistema operativo no está definida).

- Compilación del sistema operativo

  Este parámetro solo es válido para sistemas operativos Windows.

  Número de compilación del sistema operativo. Puede indicar si el número de compilación del sistema operativo seleccionado deberá ser igual, anterior o posterior al valor introducido. También puede hacer que la búsqueda incluya todos los números de compilación, excepto el especificado.

- Número de versión del sistema operativo

  Este parámetro solo es válido para sistemas operativos Windows.

  Identificador de versión del sistema operativo. Puede indicar si el sistema operativo seleccionado deberá tener un id. de versión igual, anterior o posterior al valor introducido. También puede hacer que la búsqueda incluya todos los id. de versión, excepto el especificado.

En la sección **Máquinas virtuales**, puede configurar los criterios que se usarán para incluir dispositivos en la selección basándose en el hecho de que sean máquinas virtuales o de que formen parte de una infraestructura de escritorios virtuales (VDI):

- Esta es una máquina virtual

  En la lista desplegable puede seleccionar las siguientes opciones:

  - **Sin definir**.
  - **No**. Buscar dispositivos que no sean máquinas virtuales.
  - **Sí**. Buscar dispositivos que sean máquinas virtuales.

- Tipo de máquina virtual

  En la lista desplegable, puede seleccionar el desarrollador de la máquina virtual.

  Esta lista desplegable estará disponible si seleccionó los valores **Sí** o **No es importante** en la lista desplegable **Es una máquina virtual**.

- Parte de la infraestructura de escritorio virtual

  En la lista desplegable puede seleccionar las siguientes opciones:

  - **Sin definir**.
  - **No**. Buscar dispositivos que no sean parte de la Infraestructura de escritorio virtual.
  - **Sí**. Buscar dispositivos que sean parte de una VDI.

En la sección **Registro de hardware**, puede configurar criterios para incluir dispositivos en una selección según el hardware que tengan instalado:

Asegúrese de que la utilidad lshw esté instalada en los dispositivos Linux desde los que desea obtener detalles del hardware. Los detalles de hardware obtenidos de las máquinas virtuales pueden estar incompletos según el hipervisor que se utilice.

- Dispositivo

  En la lista desplegable, puede seleccionar un tipo de unidad. Los dispositivos que tengan la unidad seleccionada se incluirán en los resultados de búsqueda.

  El campo permite realizar búsquedas de texto completo.

- Proveedor

  En la lista desplegable, puede seleccionar el nombre del fabricante de la unidad. Los dispositivos que tengan la unidad seleccionada se incluirán en los resultados de búsqueda.

  El campo permite realizar búsquedas de texto completo.

- Nombre del dispositivo

  Nombre del dispositivo en la red de Windows. El dispositivo con el nombre especificado se incluirá en la selección.

- Descripción

  Descripción del dispositivo o unidad de hardware. Los dispositivos que tengan la descripción indicada en este campo se incluirán en la selección.

  Si desea agregar una descripción a un dispositivo, puede hacerlo (en cualquier formato) a través de la ventana de propiedades del mismo. El campo permite realizar búsquedas de texto completo.

- Proveedor del dispositivo

  Nombre del fabricante del dispositivo. Los dispositivos producidos por el fabricante especificado en este campo se incluyen en la selección.

  Puede ingresar el nombre del fabricante en la ventana de propiedades de un dispositivo.

- Número de serie

Todas las unidades de hardware con el número de serie especificado en este campo se incluirán en la selección.

- **Número de inventario**

  Los equipos que tengan el número de inventario indicado en este campo se incluirán en la selección.

- **Usuario**

  Todas las unidades de hardware del usuario especificado en este campo se incluirán en la selección.

- **Ubicación**

  Ubicación de un dispositivo o una unidad de hardware (por ejemplo, en la sede central o en una sucursal). Las computadoras o dispositivos que se encuentren en la ubicación especificada en este campo se incluirán en la selección.

  Puede describir la ubicación de un dispositivo en cualquier formato en la ventana de propiedades de dicho dispositivo.

- **Velocidad de reloj de la CPU, en MHz, desde**

  La frecuencia de reloj mínima de una CPU. Los equipos cuyas CPU coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

- **Velocidad de reloj de la CPU, en MHz, hasta**

  Intervalo de frecuencias de una CPU. Los equipos cuyas CPU coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

- **Número de núcleos de CPU virtuales, desde**

  El número mínimo de núcleos de CPU virtuales. Los equipos cuyas CPU coincidan con los intervalos de núcleos virtuales especificados en estos campos de entrada (inclusive) se incluirán en la selección.

- **Número de núcleos de CPU virtuales, a**

  El número máximo de núcleos de CPU virtuales. Los equipos cuyas CPU coincidan con los intervalos de núcleos virtuales especificados en estos campos de entrada (inclusive) se incluirán en la selección.

- **Volumen del disco duro, en GB, desde**

  El volumen mínimo del disco duro en el dispositivo. Los equipos cuyos discos duros coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

- **Volumen de disco duro, en GB, hasta**

  El volumen máximo del disco duro en el dispositivo. Los equipos cuyos discos duros coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

- Tamaño de RAM, en MB, desde

  El tamaño mínimo de la memoria RAM del dispositivo. Los dispositivos cuyas RAM coincidan con el intervalo de tamaño especificado en los campos de entrada (inclusive) se incluirán en la selección.

- Tamaño de RAM, en MB, hasta

  El tamaño máximo de la RAM de los dispositivos. Los dispositivos cuyas memorias RAM coincidan con los intervalos especificados en estos campos de entrada (inclusive) se incluirán en la selección.

Detalles de software de terceros

En la sección **Registro de aplicaciones**, puede configurar los criterios para buscar dispositivos según aplicaciones instaladas en ellos:

- Nombre de la aplicación

  Lista desplegable en la que puede seleccionar una aplicación. Los dispositivos que tengan instalada la aplicación elegida se incluirán en la selección.

- Versión de la aplicación

  Campo de entrada en el que puede especificar la versión de la aplicación seleccionada.

- Proveedor

  Lista desplegable en la que puede seleccionar el desarrollador de una aplicación instalada en el dispositivo.

- Estado de la aplicación

  Lista desplegable en la que puede seleccionar el estado de la aplicación (*Instalada*, *Sin instalar*). Se incluirán en la selección los dispositivos que tengan o no tengan (dependiendo del estado seleccionado) la aplicación seleccionada.

- Buscar por actualización

  Si habilita esta opción, la búsqueda se basará en los detalles de las actualizaciones para el software instalado en los dispositivos pertinentes. Una vez que active esta casilla, los campos **Nombre de la aplicación**, **Versión de la aplicación** y **Estado de la aplicación** cambiarán a **Nombre de actualización**, **Versión de actualización** y **Estado**, respectivamente.

  Esta opción está deshabilitada de forma predeterminada.

- Nombre de la aplicación de seguridad incompatible

  Lista desplegable en la que puede seleccionar aplicaciones de seguridad de terceros. Los dispositivos que tengan instalada la aplicación seleccionada serán incluidos en la selección cuando se realice la búsqueda.

- Etiqueta de aplicación

Lista desplegable en la que puede seleccionar una etiqueta de aplicación. Se incluirán en la selección aquellos dispositivos que tengan instaladas aplicaciones que, en su descripción, contengan la etiqueta seleccionada.

- Aplicar a los dispositivos que no tengan las etiquetas especificadas

  Si habilita esta opción, la selección incluirá aquellos dispositivos que no contengan ninguna de las etiquetas seleccionadas en su descripción.

  Si deshabilita esta opción, no se aplicará el criterio.

  Esta opción está deshabilitada de forma predeterminada.

En la sección **Vulnerabilidades y actualizaciones**, puede especificar los criterios que se usarán para incluir dispositivos en la selección basándose en el origen de Windows Update que utilicen:

WUA está ahora conectado al Servidor de administración

En la lista desplegable, puede seleccionar una de las siguientes opciones de búsqueda:

- **Sí**. Si selecciona esta opción, los resultados de búsqueda incluirán aquellos dispositivos que reciban sus actualizaciones de Windows Update del Servidor de administración.
- **No**. Si selecciona esta opción, los resultados incluirán aquellos dispositivos que reciban sus actualizaciones de Windows Update de cualquier otro origen.

Detalles de las aplicaciones de Kaspersky

En la sección **Aplicaciones de Kaspersky**, puede configurar criterios para incluir dispositivos en una selección según la aplicación administrada seleccionada:

- Nombre de la aplicación

  En la lista desplegable, puede definir un criterio para incluir dispositivos en la selección cuando se realice una basada en el nombre de una aplicación de Kaspersky.

  La lista solo contendrá los nombres de aquellas aplicaciones que tengan su respectivo complemento de administración instalado en la estación de trabajo del administrador.

  Si no selecciona ninguna aplicación, este criterio no se aplicará.

- Versión de la aplicación

  En el campo de entrada, puede definir un criterio para incluir dispositivos en la selección cuando se realice una búsqueda basada en el número de versión de una aplicación de Kaspersky.

  Si no especifica un número de versión, este criterio no se aplicará.

- Nombre de la actualización crítica

Lista desplegable en la que puede seleccionar el estado de la aplicación (*Instalada*, *Sin instalar*). Se incluirán en la selección los dispositivos que tengan o no tengan (dependiendo del estado seleccionado) la aplicación seleccionada.

En el campo de entrada, puede definir un criterio para incluir dispositivos en la selección cuando se realice una búsqueda basada en el nombre de una aplicación o en un número de paquete de actualización.

Si el campo queda en blanco, este criterio no se aplicará.

- Seleccione el período de la última actualización de módulos

  Use esta opción para definir un criterio que permita buscar dispositivos según la hora en que se hayan actualizado por última vez los módulos de las aplicaciones instaladas en ellos.

  Si activa esta casilla, podrá utilizar los campos de entrada para definir el intervalo de tiempo (fecha y hora) en el que deberá haber ocurrido la última actualización de módulos de las aplicaciones instaladas en los dispositivos.

  Si no activa esta casilla, no se aplicará este criterio.

  Esta casilla no está marcada de manera predeterminada.

- El dispositivo se administra a través del Servidor de administración

  Puede usar la lista desplegable para que la selección incluya aquellos dispositivos que se administran mediante Kaspersky Security Center Cloud Console:

  - **Sí**. La selección incluirá aquellos dispositivos que se administran mediante Kaspersky Security Center Cloud Console.
  - **No**. La aplicación incluirá aquellos dispositivos que no se administran mediante Kaspersky Security Center Cloud Console.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

- La aplicación de seguridad está instalada

  Puede usar la lista desplegable para que la selección incluya aquellos dispositivos que tengan instalada la aplicación de seguridad:

  - **Sí**. La selección incluirá aquellos dispositivos en los que se haya instalado la aplicación de seguridad.
  - **No**. La selección incluirá aquellos dispositivos en los que no se haya instalado la aplicación de seguridad.
  - **Ningún valor seleccionado**. El criterio no se aplicará.

En la sección **Protección antivirus**, puede configurar los criterios para incluir dispositivos en una selección en función de su estado de protección:

- Bases de datos publicadas

Seleccione esta opción para buscar dispositivos cliente basándose en la fecha de publicación de las bases de datos antivirus. Utilice el campo de entrada para definir el intervalo de tiempo que se tomará como base para la búsqueda.

Esta opción está deshabilitada de forma predeterminada.

- Registros de la base de datos

  Si se habilita esta opción, podrá buscar los dispositivos cliente por el número de registros de la base de datos. En los campos de entrada puede establecer los valores umbral más bajos y más altos de los registros de la base de datos antivirus.

  Esta opción está deshabilitada de forma predeterminada.

- Último análisis

  Habilite esta opción para buscar dispositivos cliente basándose en la hora del último análisis antimalware. Utilice los campos de entrada para definir el período en el cual deberá haber ocurrido el último análisis antimalware.

  Esta opción está deshabilitada de forma predeterminada.

- Amenazas detectadas

  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 forma predeterminada.

La subsección **Componentes de las aplicaciones** contiene la lista de componentes de aquellas aplicaciones que tienen los complementos de administración correspondientes instalados en Kaspersky Security Center Cloud Console.

En la sección **Componentes de las aplicaciones**, puede definir criterios para incluir dispositivos en la selección basándose en los estados y los números de versión de los componentes vinculados a la aplicación seleccionada:

- Estado

Buscar dispositivos basándose en el estado de un componente reportado por una aplicación al Servidor de administración. Puede seleccionar uno de los siguientes estados: *N/D, Detenido*, *En pausa*, *Iniciándose*, *En ejecución, Error, Sin instalar, No compatible con la licencia*. Si el componente seleccionado de la aplicación instalada en un dispositivo administrado tiene el estado especificado, el dispositivo será incluido en la selección de dispositivos.

Estados reportados por las aplicaciones:

- *Detenido*: el componente está deshabilitado y no se encuentra en funcionamiento.
- *En pausa*: el componente se encuentra suspendido (por ejemplo, porque el usuario pausó la protección en la aplicación administrada).
- *Iniciándose*: el componente está en proceso de iniciarse.
- *En ejecución*: el componente está habilitado y funciona correctamente.
- *Error*: ocurrió un error durante el funcionamiento del componente.
- *Sin instalar*: el usuario no optó por instalar el componente al realizar una instalación personalizada de la aplicación.
- *No compatible con la licencia*: la licencia no cubre el componente seleccionado.

A diferencia de los demás estados, *N/D* no es un estado reportado por las aplicaciones. Se trata de una opción que muestra que las aplicaciones no tienen información sobre el estado del componente seleccionado. Esta situación puede presentarse, por ejemplo, cuando el componente seleccionado no pertenece a ninguna de las aplicaciones instaladas en el dispositivo o cuando el dispositivo está apagado.

- **Versión**

Buscar dispositivos basándose en el número de versión del componente seleccionado en la lista. Puede escribir un número de versión (por ejemplo, `3.4.1.0`) y luego especificar si 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 forma predeterminada.

Para agregar etiquetas al criterio, haga clic en el botón **Agregar** y seleccione las etiquetas haciendo clic en el campo de entrada **Etiqueta**. Especifique si desea incluir o excluir los dispositivos con las etiquetas seleccionadas en la selección de dispositivos.

- **Todos los dispositivos que tengan esta etiqueta**

  Si selecciona esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que lleven, en su descripción, la etiqueta seleccionada. La consulta de búsqueda puede incluir el asterisco, que representa una cadena de cualquier longitud (número de caracteres).

  Esta opción está seleccionada de manera predeterminada.

- **Todos los dispositivos que no tengan esta etiqueta**

  Si selecciona esta opción, los resultados de búsqueda mostrarán aquellos dispositivos que no lleven en su descripción la etiqueta seleccionada. La consulta de búsqueda puede incluir el asterisco, que representa una cadena de cualquier longitud (número de caracteres).

Usuarios

En la sección **Usuarios**, puede configurar los criterios para incluir dispositivos en la selección basándose en las cuentas de usuario con las que se haya iniciado sesión en el sistema operativo.

- **Último usuario que inició sesión en el sistema**

  Si esta opción está habilitada, puede seleccionar la cuenta de usuario para configurar el criterio. Tenga en cuenta que la lista de usuarios está filtrada y muestra los usuarios internos. Los resultados de la búsqueda incluyen los dispositivos en los que el usuario seleccionado realizó 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 está filtrada y muestra los usuarios internos. Los resultados de la búsqueda incluyen 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 una selección de dispositivos, haga lo siguiente:

1. Abra la tabla de dispositivos de la selección de dispositivos como se indica más arriba.
2. Utilice una de las siguientes formas para seleccionar los dispositivos que desea exportar:
   - Para seleccionar dispositivos específicos, seleccione las casillas de verificación junto a ellos.
   - Para seleccionar todos los dispositivos de la página de la tabla actual, seleccione la casilla de verificación en el encabezado de la tabla de dispositivos y luego seleccione la casilla de verificación **Seleccionar todo en la página actual**.
   - Para seleccionar todos los dispositivos de la tabla, seleccione la casilla de verificación en el encabezado de la tabla de dispositivos y luego seleccione la casilla de verificación **Seleccionar todo**.

Haga clic en el botón **Exportar a CSV** o **Exportar a TXT**. Se exportará toda la información sobre los dispositivos seleccionados incluidos en la tabla.

Tenga en cuenta que si aplicó un criterio de filtro a la tabla de dispositivos, solo se exportarán los datos filtrados de las columnas mostradas.

Eliminación de dispositivos de los grupos de administración en una selección

Cuando se trabaja con la selección de dispositivos, puede eliminar los dispositivos de los grupos de administración en la misma selección, sin cambiar a los grupos de administración de los que se deben eliminar estos dispositivos.

Para eliminar los dispositivos de los grupos de administración:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Selecciones de dispositivos** o a la sección **Descubrimiento y despliegue** → **Selecciones de dispositivos**.
2. En la lista de selecciones, haga clic en el nombre de la selección de dispositivos.

   La página muestra una tabla con información sobre los dispositivos incluidos en la selección de dispositivos.
3. Seleccione los dispositivos que desee eliminar y, a continuación, haga clic en **Eliminar**.

   Los dispositivos seleccionados se quitarán de los grupos de administración correspondientes.

Ver y configurar las acciones para dispositivos inactivos

Puede recibir una notificación si se detecta que los dispositivos cliente de un grupo están inactivos. También puede hacer que esos dispositivos se eliminen automáticamente.

Para ver o configurar las acciones que se llevan a cabo cuando los dispositivos de un grupo están inactivos:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. Haga clic en el nombre del grupo de administración de su interés.

   Se abrirá la ventana de propiedades del grupo de administración.
3. En la ventana de propiedades, vaya a la pestaña **Configuración**.
4. En la sección **Herencia**, active o desactive las siguientes opciones:

   - Heredar del grupo primario

     La configuración de la sección se heredará del grupo primario al que pertenezca el dispositivo cliente. Si esta opción está habilitada, los ajustes de la sección **Actividad de los dispositivos en la red** no se podrán modificar.

     Para que esta opción esté disponible, el grupo de administración debe tener un grupo primario.

     Esta opción está activada de forma predeterminada.

- Forzar la herencia de configuración en los grupos secundarios

  Los valores de configuración se propagarán a los grupos secundarios. Los ajustes correspondientes estarán bloqueados en las propiedades de esos grupos.

  Esta opción está deshabilitada de forma predeterminada.

5. En la sección **Actividad de los dispositivos**, active o deshabilite las siguientes opciones:

- Notificar al administrador si el dispositivo ha estado inactivo por más de (días)

  Cuando esta opción está habilitada y se detecta que un dispositivo ha estado inactivo, el administrador recibe una notificación. Puede especificar el intervalo de tiempo que se deja pasar antes de que se cree el evento **El dispositivo ha estado inactivo en la red por mucho tiempo**. El intervalo de tiempo por defecto es de 7 días.

  Esta opción está activada de forma predeterminada.

- Eliminar el dispositivo del grupo si ha estado inactivo por más de (días)

  Si esta opción está habilitada, puede especificar el intervalo de tiempo que se deja pasar antes de que el dispositivo se elimine del grupo automáticamente. El intervalo de tiempo por defecto es de 60 días.

  Esta opción está activada de forma predeterminada.

6. Haga clic en **Guardar**.

Se guardarán y aplicarán los cambios.

Acerca de los estados de los dispositivos

Kaspersky Security Center 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 en la red del dispositivo (vea la tabla de más abajo). 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*
- *Sin inconvenientes* o *Sin inconvenientes/Visible*

En la siguiente tabla, se enumeran las condiciones predeterminadas que se deben cumplir para que se asignen los estados *Crítico* o *Advertencia* a un dispositivo, con todos los valores posibles.

Condiciones para que se asigne un estado a un dispositivo

Condición	Descripción de la condición	Valores disponibles
La aplicación de seguridad no está instalada	El Agente de red está instalado en el dispositivo, pero no hay una aplicación de seguridad instalada.	• Interruptor activado.

		• Interruptor desactivado.
Se detectaron demasiados virus	Una tarea de detección de virus (por ejemplo, la tarea "Análisis antivirus") ha detectado virus en el dispositivo y el número de virus encontrados supera el valor especificado.	Más de 0.
El nivel de protección en tiempo real difiere del nivel establecido por el administrador	El dispositivo es visible en la red, pero el nivel de la protección en tiempo real no se corresponde con el que el administrador configuró (en la condición) para el estado del dispositivo.	• Detenida. • En pausa. • En ejecución.
No se ha realizado un análisis antimalware en mucho tiempo	El dispositivo está visible en la red y tiene instalada una aplicación de seguridad, pero la tarea *Análisis antimalware* no se ha ejecutado en el intervalo de tiempo especificado. Esta condición se aplica solo a los dispositivos que se agregaron al menos siete días antes a la base de datos del Servidor de administración.	Más de 1 día.
Las bases de datos están desactualizadas	El dispositivo es visible en la red y tiene instalada una aplicación de seguridad, pero sus bases de datos antivirus no se han actualizado en el período de tiempo especificado. Esta condición se aplica solo a los dispositivos que se agregaron al menos un día antes a la base de datos del Servidor de administración.	Más de 1 día.
Sin conexión desde hace mucho tiempo	El Agente de red está instalado en el dispositivo, pero el dispositivo está apagado y no se ha conectado a un Servidor de administración durante el período de tiempo especificado.	Más de 1 día.
Se han detectado amenazas activas	El número de objetos no procesados en la carpeta **Amenazas activas** supera el valor especificado.	Más de 0 elementos.
Se debe reiniciar el dispositivo	El dispositivo es visible en la red, pero una aplicación requiere que el dispositivo se reinicie por más tiempo que el intervalo de tiempo especificado y por una de las razones seleccionadas.	Más de 0 minutos.
Hay aplicaciones incompatibles instaladas	El dispositivo es visible en la red, pero, al hacer un inventario de software a través del Agente de red, se detectaron aplicaciones incompatibles instaladas en el dispositivo.	• Interruptor desactivado. • Interruptor activado.
Se detectaron vulnerabilidades de software	El dispositivo es visible en la red y tiene instalado el Agente de red, pero la tarea *Buscar vulnerabilidades y actualizaciones requeridas* ha encontrado aplicaciones instaladas en el dispositivo que tienen vulnerabilidades con el nivel de gravedad especificado.	• Crítico. • Alto. • Medio. • Ignorar si la vulnerabilidad no se puede reparar. • Ignorar si hay una actualización asignada para instalarse.
Licencia caducada	El dispositivo es visible en la red, pero la licencia ha caducado.	• Interruptor desactivado. • Interruptor activado.
La licencia está por caducar	El dispositivo es visible en la red, pero la licencia instalada en el mismo caduca en menos días que el número de días especificado.	Más de 0 días.
La búsqueda de actualizaciones de Windows Update no se ha realizado en mucho tiempo	El dispositivo es visible en la red, pero la tarea "Sincronización con Windows Update" no se ha ejecutado en el período 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 con la directiva	Los ajustes del dispositivo móvil no son los que se encontraron en la directiva de Kaspersky Endpoint Security para Android durante el chequeo de reglas de cumplimiento normativo.	• Interruptor desactivado. • Interruptor activado.
Problemas de seguridad no procesados detectados	Se han encontrado problemas de seguridad sin procesar en el dispositivo. Los problemas de seguridad se pueden crear manualmente por el administrador o automáticamente por las aplicaciones de Kaspersky administradas que se han instalado en el dispositivo cliente.	• Interruptor desactivado. • 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 en el disco	El espacio libre en el disco del dispositivo es inferior al valor especificado o el dispositivo no se pudo sincronizar con el Servidor de administración. Los estados *Crítico* o *Advertencia* cambiarán por el estado *Sin inconvenientes* cuando el dispositivo se sincronice correctamente con el Servidor de administración y el espacio libre en el dispositivo supere o iguale el valor especificado.	Más de 0 MB.
El dispositivo ha cambiado a no administrado	Durante el descubrimiento de dispositivos, el dispositivo se reconoció como visible en la red, pero hubo más de tres intentos de sincronizar el dispositivo con el Servidor de administración que terminaron con un error.	• Interruptor desactivado. • Interruptor activado.
Protección deshabilitada	El dispositivo es visible en la red, pero la aplicación de seguridad del dispositivo ha estado deshabilitada por un tiempo superior al especificado. En este caso, el estado de la aplicación de seguridad es *detenida* o *error*, y difiere del siguiente: *iniciada*, *en ejecución* o *suspendida*.	Más de 0 minutos.
La aplicación de seguridad no está en ejecución	El dispositivo es visible en la red y tiene instalada una aplicación de seguridad, pero esa aplicación no se está ejecutando.	• Interruptor desactivado. • Interruptor activado.

Kaspersky Security Center Cloud Console permite que, en respuesta a determinadas condiciones, se modifique automáticamente el estado de un dispositivo agregado a un grupo de administración. 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*.

A la hora de asignar un estado a un dispositivo, para algunas condiciones (vea la columna "Descripción de la condición"), Kaspersky Security Center Cloud Console 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 **Fijar en Crítico si esto se cumple**, habilite la condición bajo la cual el estado de un dispositivo cambiará a *Crítico*.

   Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.

6. En la lista, seleccione el botón de opción ubicado junto a la condición.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor necesario para la condición seleccionada.

   No es posible configurar valores para todas las condiciones.
9. Haga clic en **Aceptar**.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Crítico* al dispositivo administrado.

Para habilitar el cambio de estado a Advertencia para los dispositivos:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.

2. En la lista de grupos que se abre, haga clic en el vínculo con el nombre del grupo que contenga los dispositivos para los que desee modificar el cambio de estado.

3. En la ventana de las propiedades que se abre, seleccione la pestaña **Estado del dispositivo**.

4. En el panel izquierdo, seleccione **Advertencia**.

5. En el panel derecho, en la sección **Fijar en Advertencia si esto se cumple**, habilite la condición que hará que el estado de un dispositivo cambie a *Advertencia*.

   Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.

6. En la lista, seleccione el botón de opción ubicado junto a la condición.

7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.

8. Configure el valor necesario para la condición seleccionada.

   No es posible configurar valores para todas las condiciones.

9. Haga clic en **Aceptar**.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Advertencia* al dispositivo administrado.

Cambiar los dispositivos cliente de Servidor de administración

Puede cambiar el Servidor de administración que administra los dispositivos cliente por otro, mediante la tarea **Cambiar Servidor de administración**. 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 **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En el paso **Configuración de tarea nueva**, 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 la tarea se asigna a un grupo de administración, la pestaña **Seguridad** no se mostrará en la ventana de propiedades de la tarea; esto se debe a que las tareas de grupo están sujetas a la configuración de seguridad de los grupos a los que se aplican.

- Especificar las direcciones de los dispositivos manualmente o importarlas de una lista

  Puede especificar nombres de NetBIOS, nombres de DNS, direcciones IP y subredes IP de los dispositivos a los cuales debe asignar la tarea.

  Podría elegir esta opción si necesita que la tarea se ejecute en una subred específica. Esto puede ser útil si, por ejemplo, necesita instalar una aplicación solo en los dispositivos que utilizan los contadores o si quiere analizar los dispositivos de una subred puntual que probablemente esté infectada.

- Asignar tarea a una selección de dispositivos

  La tarea se asignará a los dispositivos incluidos en una selección de dispositivos. Puede elegir una selección existente.

  Esta opción puede ser útil para, por ejemplo, ejecutar una tarea en los dispositivos que tengan una versión específica de un sistema operativo.

4. En el paso **Alcance de la tarea**, indique 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 **Seleccione una cuenta con la que 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 forma predeterminada.

- Especificar cuenta

  Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

- Cuenta

Cuenta con la que se ejecutará la tarea.

- **Contraseña**

  Contraseña de la cuenta con la que se ejecutará la tarea.

8. Si habilita la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**, 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 habilitar la opción **Instalar solo en dispositivos administrados a través de este Servidor de administración** en las propiedades de la tarea *Instalar aplicación de forma remota*.

Si habilita la opción **Instalar solo en dispositivos administrados a través de este Servidor de administración** y luego ejecuta la tarea *Instalar aplicación de forma remota*, se realiza una verificación para determinar si los dispositivos están administrados por otro Servidor de administración. Para los dispositivos administrados por otro Servidor de administración, el valor del atributo **Administrado por un Servidor de administración diferente** se establecerá en `true`. La tarea *Instalar aplicación de forma remota* no se aplicará a estos dispositivos.

Los valores del atributo **Administrado por un Servidor de administración diferente** se muestran en la columna **Administrado por un Servidor de administración diferente** en la lista de dispositivos administrados y la lista de dispositivos no asignados.

También puede usar la propiedad **Administrado por un Servidor de administración diferente** como criterio para los siguientes propósitos:

- Mostrar dispositivos administrados

- Selecciones de dispositivos
- Reglas de movimiento de dispositivos
- Reglas de etiquetado automático

Para restablecer el atributo Administrado por un Servidor de administración diferente,

En el menú principal de Kaspersky Security Center Cloud Console, vaya a **Descubrimiento 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 un Servidor de administración diferente**.

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:

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, haga clic 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, haga clic en el nombre del dispositivo. En la ventana que se abre, vaya a la pestaña **Aplicaciones** y 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 del **Servidor de administración doméstico** y del **Modo sin conexión**.
4. Haga clic en el botón **Agregar** y, en la ventana que se abre, especifique el nombre del perfil.

   El nombre debe ser único. No puede usar el mismo nombre para varios perfiles.
5. Si es necesario, seleccione las casillas de los siguientes campos:
   - **Habilitar el modo de fuera de la oficina cuando el Servidor de administración no esté disponible**.

- **Usar servidor proxy**.

  Si selecciona esta opción, haga lo siguiente:

  - Especifique la información en los campos **Dirección** y **Número de puerto**.
  - Si es necesario, seleccione la casilla **Autenticación del servidor proxy** y especifique el nombre de usuario y la contraseña en los campos correspondientes.

6. Haga clic en el botón **Guardar**.

El nuevo perfil se muestra en la tabla de perfiles de conexión. Puede usarlo para establecer la **Configuración de ubicación de red**.

La configuración de una ubicación de red define las características de la red con la cual está conectado el dispositivo cliente y especifica las reglas que hacen que el Agente de red cambie de un perfil de conexión de Servidor de administración a otro en respuesta a un cambio en las características de la red.

Puede editar y eliminar perfiles de conexión.

Para editar un perfil de conexión:

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 haga clic en el botón **Guardar**.

   Los cambios se aplican al perfil de conexión.

Para eliminar un perfil de conexión:

1. En la tabla de perfiles de conexión, seleccione las casillas de verificación junto a los perfiles de conexión que desea eliminar.
2. Haga clic en el botón **Eliminar**.

   Se eliminan los perfiles de conexión seleccionados.

Sobre clústeres y conjuntos de servidores

Kaspersky Security Center Cloud Console es compatible con 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 conjuntos de servidores, la página **Dispositivos administrados** muestra dos pestañas: una para dispositivos individuales y otra para clústeres y conjuntos de servidores. Una vez que los dispositivos administrados se detectan como nodos de clúster, el clúster se agrega como un objeto individual a la pestaña **Clústeres y conjuntos de servidores**.

Los nodos de los clústeres o conjuntos de servidores se enumeran en la pestaña **Dispositivos**, junto con otros dispositivos administrados. Puede ver las propiedades de los nodos como dispositivos individuales y llevar a cabo otras operaciones, pero no puede eliminar un nodo de clúster ni moverlo a otro grupo de administración por separado de su clúster. Solo puede eliminar o mover un clúster completo.

Puede realizar las siguientes operaciones con clústeres o conjuntos de servidores:

- Ver las propiedades
- Mover el clúster o conjunto de servidores a otro grupo de administración

  Cuando mueve un clúster o un conjunto de servidores a otro grupo, todos sus nodos se mueven con él, porque un clúster y cualquiera de sus nodos siempre pertenecen al mismo grupo de administración.
- Eliminar

  Es razonable eliminar un clúster o un conjunto de servidores solo cuando el clúster o conjunto de servidores ya no existe en la red de la organización. Si un clúster aún está visible en su red y el Agente de red y la aplicación de seguridad de Kaspersky todavía están instalados en los nodos del clúster, Kaspersky Security Center Cloud Console devuelve el clúster eliminado y sus nodos a la lista de dispositivos administrados de manera automática.

Propiedades de un clúster o conjunto de servidores

Para ver la configuración de un clúster o conjunto de servidores:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados** → **Clústeres y conjuntos de servidores**.

   Se muestra la lista de clústeres y conjuntos de servidores.
2. Haga clic en el nombre del clúster o conjunto de servidores requerido.

Se muestra la ventana de propiedades del clúster o conjunto de servidores seleccionado.

General

La sección **General** muestra información general sobre el clúster o conjunto de servidores. La información se basa en los datos recibidos durante la última sincronización de los nodos del clúster con el Servidor de administración.

- **Nombre**
- **Descripción**
- **Dominio de Windows**

  Dominio o grupo de trabajo de Windows, que contiene el clúster o conjunto de servidores.
- **Nombre NetBIOS**

  Nombre de red de Windows del clúster o conjunto de servidores.
- **Nombre DNS**

  Nombre del dominio DNS del clúster o conjunto de servidores.

Tareas

La pestaña **Tareas** permite administrar las tareas del clúster o conjunto de servidores. Utilice esta sección para crear tareas nuevas, ver la lista de tareas existentes, ver los resultados de ejecución de las tareas e iniciar, detener, eliminar y reconfigurar las tareas existentes. Las tareas enumeradas se relacionan con la aplicación de seguridad de Kaspersky instalada en los nodos del clúster. Kaspersky Security Center Cloud Console recibe la lista de tareas y los detalles del estado de las tareas de los nodos del clúster. Si no se puede establecer una conexión, no se mostrará ningún estado.

Nodos

Esta pestaña muestra una lista de nodos incluidos en el clúster o conjunto de servidores. Puede hacer clic en el nombre de un nodo para ver la ventana de propiedades del dispositivo.

Aplicación de Kaspersky

La ventana de propiedades también puede contener pestañas adicionales con información y configuraciones relacionadas con la aplicación de seguridad de Kaspersky instalada en los nodos del clúster.

Etiquetas de dispositivo

Kaspersky Security Center Cloud Console le permite etiquetar dispositivos. Las *etiquetas* son rótulos que se asignan a los dispositivos para describirlos, agruparlos y encontrarlos. 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. El etiquetado automático es un proceso realizado por Kaspersky Security Center Cloud Console siguiendo reglas de etiquetado específicas.

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. A modo de ejemplo, si tiene dispositivos con Windows, Linux y macOS en su red, puede configurar una regla que asigne la etiqueta `[Linux]` a todos los dispositivos con Linux. Podrá usar esa etiqueta para crear una selección de dispositivos, ayudarse a clasificar los dispositivos con Linux y asignar a los mismos 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 **Agregar**.

   Se abre una ventana para crear la etiqueta.

3. En el campo **Etiqueta**, escriba el nombre de la etiqueta.

4. Haga clic en **Guardar** para guardar los cambios.

La nueva etiqueta aparece en la lista de etiquetas de dispositivo.

Cambiar el nombre de una etiqueta de dispositivo

Para cambiar el nombre de una etiqueta de dispositivo:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Etiquetas** → **Etiquetas 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 la etiqueta del dispositivo, use la utilidad klscflag.

Ver los dispositivos que tienen asignada una etiqueta

Para ver cuáles dispositivos tienen asignada una etiqueta:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Etiquetas** → **Etiquetas 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 **Modo de asignación**, 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 usando 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 **Agregar**.
3. En la ventana que se abre, realice una de las siguientes acciones:

- Para crear y asignar una nueva etiqueta, seleccione **Crear nueva etiqueta** y luego escriba el nombre de la nueva etiqueta.
- Para seleccionar una etiqueta existente, seleccione **Asignar etiqueta existente** y luego, en la lista desplegable, elija la etiqueta pertinente.

4. Haga clic en **Aceptar** para aplicar los cambios.
5. Haga clic en **Guardar** para guardar los cambios.

La etiqueta seleccionada se asigna al dispositivo.

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.
   También puede hacer lo siguiente:
   - Edite el nombre de una etiqueta haciendo clic en el ícono **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 ícono **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. Marque la casilla de verificación adyacente a la etiqueta que desee quitar del dispositivo.
5. Al principio de la lista, haga clic en el botón **¿Desea desasignar la etiqueta?**.
6. En la ventana que se abre, haga clic en **Sí**.

El dispositivo pierde la etiqueta.

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 una de las siguientes acciones:

- En el menú principal, vaya a **Activos (dispositivos)** → **Etiquetas** → **Reglas de etiquetado automático**.
- En el menú principal, vaya a **Activos (dispositivos)** → **Etiquetas** → **Etiquetas de dispositivos** y luego haga clic en el vínculo **Configurar reglas de etiquetado automático**.
- Vea las etiquetas asignadas a un dispositivo y después haga clic en el botón **Configuración**.

Se mostrará una lista con las reglas de etiquetado automático de dispositivos.

Modificación de una regla para etiquetar dispositivos automáticamente

Para modificar una regla para etiquetar dispositivos automáticamente:

1. Vea las reglas de etiquetado automático de dispositivos.

2. Haga clic en el nombre de la regla que desee editar.

   Se abre una ventana para configurar la regla.

3. Modifique las propiedades generales de la regla:

   a. En el campo **Nombre de la regla**, cambie el nombre de regla.

      El nombre no puede contener más de 256 caracteres.

   b. Realice una de las siguientes acciones:

      - Pase el interruptor a **Regla habilitada** para habilitar la regla.
      - Pase el interruptor a **Regla deshabilitada** para deshabilitar la regla.

4. Realice una de las siguientes acciones:

   - Si desea agregar una condición, haga clic en el botón **Agregar** y, en la ventana que se abre, especifique la configuración de la nueva condición.
   - Si desea editar una condición existente, haga clic en el nombre de la condición que desee modificar y, a continuación, edite la configuración de la condición.
   - Si desea eliminar una condición, marque la casilla adyacente al nombre de la condición que desee eliminar y haga clic en **Eliminar**.

5. Haga clic en **Aceptar** en la ventana de configuración de condiciones.

6. Haga clic en **Guardar** para guardar los cambios.

La regla modificada se muestra en la lista.

Creación de una regla para etiquetar dispositivos automáticamente

Para crear una regla para etiquetar dispositivos automáticamente:

1. Vea las reglas de etiquetado automático de dispositivos.

2. Haga clic en **Agregar**.

   Se abre una ventana para configurar la nueva regla.

3. Configure las propiedades generales de la regla:

   a. En el campo **Nombre de la regla**, escriba el nombre de la regla.

      El nombre no puede contener más de 256 caracteres.

   b. Realice una de las siguientes acciones:

      - Pase el interruptor a **Regla habilitada** para habilitar la regla.
      - Pase el interruptor a **Regla deshabilitada** para deshabilitar la regla.

   c. En el campo **Etiqueta**, escriba el nombre de una nueva etiqueta de dispositivo o seleccione una etiqueta de dispositivo de la lista.

El nombre no puede contener más de 256 caracteres.

4. En la sección de condiciones, haga clic en el botón **Agregar** para añadir una nueva condición.

   Se abre una ventana para configurar la nueva condición.

5. Escriba el nombre de la condición.

   El nombre no puede contener más de 256 caracteres. No puede haber más de una condición con el mismo nombre dentro de una regla.

6. Configure las condiciones de activación de la regla. Puede seleccionar varias condiciones.

   - **Red**: atributos de red del dispositivo (por ejemplo, el nombre del dispositivo en la red de Windows o su pertenencia a un dominio o a una subred IP).

     Si la intercalación con diferenciación entre mayúsculas y minúsculas está configurada para la base de datos utilizada para Kaspersky Security Center Cloud Console, respete las mayúsculas y minúsculas cuando ingrese el nombre DNS de un dispositivo. De lo contrario, la regla de etiquetado automático no funcionará.

   - **Aplicaciones**: presencia del Agente de red en el dispositivo, tipo y versión de sistema operativo, arquitectura del sistema operativo.
   - **Máquinas virtuales**: el hecho de que el dispositivo corresponda a un tipo concreto de máquina virtual.
   - **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. Marque la casilla ubicada junto a la regla que desee eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic de nuevo en **Eliminar**.

Se elimina la regla seleccionada. La etiqueta especificada en las propiedades de la regla se desasigna de los dispositivos que la tenían asignada.

La etiqueta desasignada no se elimina. Si lo desea, puede eliminarla manualmente.

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 genera una lista sumaria de los archivos movidos a Cuarentena o a Copia de seguridad por las aplicaciones de Kaspersky instaladas 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 los archivos de estos repositorios al Servidor de administración. Los archivos quedan almacenados en los repositorios de los dispositivos.

Descargar archivos de los repositorios

Kaspersky Security Center Cloud Console permite descargar copias de los archivos que la aplicación de seguridad de un dispositivo cliente ha colocado en Cuarentena o en Copia de seguridad. Los archivos descargados se guardan en una ubicación elegida por usted.

Para poder descargar archivos, se debe cumplir alguna de estas condiciones: la opción **No desconectar del Servidor de administración** debe estar habilitada en la configuración del dispositivo o se debe estar usando un servidor push o una puerta de enlace de conexión. Si no se cumplen estas condiciones, no podrá realizar la descarga.

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.

En el dispositivo cliente, la aplicación de seguridad que haya puesto los archivos en el repositorio (Cuarentena o Copia de seguridad) los eliminará del mismo.

Diagnóstico remoto de dispositivos cliente

Puede usar la función de diagnóstico remoto para realizar a distancia las siguientes operaciones en dispositivos cliente basados en Windows y Linux:

- Habilitar y deshabilitar la característica de seguimiento, cambiar el nivel de seguimiento y descargar el archivo de seguimiento
- Descargar información del sistema y los ajustes de las aplicaciones
- Descargar registros de eventos
- Crear un archivo de volcado para una aplicación
- Realizar un diagnóstico y descargar el informe de diagnóstico
- Iniciar, detener y reiniciar aplicaciones

Puede utilizar los registros de eventos y los informes de diagnóstico descargados de un dispositivo cliente para solucionar problemas por cuenta propia. Si se comunica con el servicio de soporte técnico de Kaspersky, los especialistas podrían pedirle que descargue archivos de seguimiento, archivos de volcado, registros de eventos e informes de diagnóstico del dispositivo cliente para que sean analizados en Kaspersky.

Abrir la ventana de diagnóstico remoto

Para realizar un diagnóstico remoto de dispositivos cliente basados en Windows y Linux, debe abrir la ventana de diagnóstico remoto.

Para abrir la ventana de diagnóstico remoto:

1. Realice una de las siguientes acciones para seleccionar el dispositivo para el que desee abrir la ventana de diagnóstico remoto:
   - Si el dispositivo pertenece a un grupo de administración, en el menú principal, vaya a **Activos (dispositivos)** → **Grupos** → **<nombre del grupo>** → **Dispositivos administrados**.
   - Si el dispositivo pertenece al grupo Dispositivos no asignados, en el menú principal, vaya a **Descubrimiento y despliegue** → **Dispositivos no asignados**.
2. Haga clic en el nombre del dispositivo pertinente.
3. En la ventana que se abre, que contendrá las propiedades del dispositivo, elija la pestaña **Avanzado**.
4. En la pestaña **Avanzado**, haga clic en **Diagnóstico remoto**.

Esto abre la ventana **Diagnóstico remoto** de un dispositivo cliente. Si no se establece la conexión entre el Servidor de administración y el dispositivo cliente, se muestra el mensaje de error.

Como alternativa, si necesita obtener toda la información de diagnóstico sobre un dispositivo cliente basado en Linux a la vez, puede ejecutar el script collect.sh en este dispositivo.

Habilitar y deshabilitar el seguimiento para las aplicaciones

Puede habilitar y deshabilitar el seguimiento para las aplicaciones, incluido el seguimiento con Xperf.

Habilitar y deshabilitar el seguimiento

Para habilitar o deshabilitar el seguimiento en un dispositivo remoto:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
3. En la lista de aplicaciones, seleccione la aplicación para la que desee habilitar o deshabilitar el seguimiento.

   Se abre la lista de opciones de diagnóstico remoto.
4. Si desea habilitar el seguimiento, haga lo siguiente:

   a. En la sección **Seguimiento**, haga clic en **Habilitar seguimiento**.

   b. En la ventana **Modificar nivel de seguimiento**, recomendamos que mantenga los valores de configuración predeterminados. De ser necesario, un especialista del servicio de soporte técnico le indicará cómo modificar la configuración. Las opciones de configuración disponibles son las siguientes:

   - **Nivel de seguimiento**

     El nivel de seguimiento determina qué tan detallado es el archivo de seguimiento.

   - **Seguimiento con rotación**

     La información de seguimiento se sobrescribe para que el archivo de seguimiento no aumente de tamaño desmedidamente. Especifique el número máximo de archivos que se utilizarán para almacenar la información de seguimiento y el tamaño máximo de cada archivo. Una vez que se haya guardado el número máximo de archivos de seguimiento, cada cual con su tamaño máximo, se eliminará el archivo de seguimiento más antiguo para que se pueda guardar un nuevo archivo de seguimiento.

     Esta opción solo está disponible para Kaspersky Endpoint Security.

   c. Haga clic en **Guardar**.

Se habilita el seguimiento para la aplicación seleccionada. En algunos casos, para habilitar el seguimiento, deberá reiniciar la aplicación de seguridad y su tarea.

En los dispositivos cliente basados en Linux, el seguimiento del componente Actualizador del agente de Kaspersky Security se regula mediante la configuración del Agente de red. Por lo tanto, las opciones **Habilitar seguimiento** y **Modificar nivel de seguimiento** están deshabilitadas para este componente en dispositivos cliente que ejecutan Linux.

5. Para deshabilitar el seguimiento para la aplicación seleccionada, haga clic en **Deshabilitar seguimiento**.

   Se deshabilita el seguimiento para la aplicación seleccionada.

Habilitar el seguimiento con Xperf

Si utiliza Kaspersky Endpoint Security, un especialista de nuestro servicio de soporte técnico podría pedirle que habilite el seguimiento con Xperf. Esta función permite obtener información sobre el rendimiento del sistema.

Para habilitar y configurar el seguimiento con Xperf o deshabilitarlo, siga los siguientes pasos:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.

2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.

3. En la lista de aplicaciones, seleccione Kaspersky Endpoint Security para Windows.

   Se muestra la lista de opciones de diagnóstico remoto para la app Kaspersky Endpoint Security para Windows.

4. En la sección **Seguimiento con Xperf**, haga clic en **Habilitar seguimiento con Xperf**.

   Si el seguimiento con Xperf ya está habilitado, verá, en cambio, el botón **Deshabilitar seguimiento con Xperf**. Haga clic en este botón si desea deshabilitar el seguimiento con Xperf para Kaspersky Endpoint Security para Windows.

5. Cuando se abra la ventana **Cambiar el nivel de seguimiento con Xperf**, dependiendo de lo que le haya pedido el especialista en soporte técnico, haga lo siguiente:

   a. Seleccione uno de los siguientes niveles de seguimiento:

   - **Nivel bajo**

     Un archivo de seguimiento de este tipo contiene una cantidad mínima de información sobre el sistema.

     Esta opción está seleccionada de forma predeterminada.

   - **Nivel profundo**

     Un archivo de seguimiento de este tipo contiene información más detallada que los archivos de seguimiento que se generan cuando se elige la opción *Nivel bajo*. El especialista en soporte técnico podría pedirle que elija este nivel si la información contenida en un archivo de nivel bajo no basta para evaluar el rendimiento del sistema. Un archivo de seguimiento de *Nivel profundo* contiene distintas clases de información técnica sobre el sistema: información sobre el hardware, el sistema operativo, la lista de procesos y programas iniciados y finalizados, los eventos utilizados para la evaluación del rendimiento, eventos de la Herramienta de evaluación del sistema de Windows y más.

   b. Seleccione uno de los siguientes tipos de seguimiento con Xperf:

- **Tipo básico**

  La información de seguimiento se obtendrá mientras Kaspersky Endpoint Security esté en funcionamiento.

  Esta opción está seleccionada de forma predeterminada.

- **Tipo con reinicio**

  La información de seguimiento se obtendrá cuando se inicie el sistema operativo del dispositivo administrado. Este tipo de seguimiento es efectivo cuando el problema que afecta al rendimiento del sistema ocurre después de encender el dispositivo y antes de que se inicie Kaspersky Endpoint Security.

También podrían pedirle que habilite la opción **Tamaño de archivos de rotación, en MB** para evitar que el archivo de seguimiento aumente de tamaño desmedidamente. Si habilita esta opción, especifique el tamaño que el archivo de seguimiento podrá tener como máximo. Cuando el archivo alcance su máximo tamaño, la información de seguimiento más antigua comenzará a reemplazarse con información nueva.

c. Defina el tamaño del archivo de rotación.

d. Haga clic en **Guardar**.

El seguimiento con Xperf queda configurado y habilitado.

6. Si desea deshabilitar el seguimiento con Xperf para Kaspersky Endpoint Security para Windows, haga clic en **Deshabilitar seguimiento con Xperf** en la sección **Seguimiento con Xperf**.

   Se deshabilita el seguimiento con Xperf.

Descargar los archivos de seguimiento de una aplicación

Para poder descargar archivos de seguimiento de un dispositivo cliente, se debe cumplir alguna de estas condiciones: la opción **No desconectar del Servidor de administración** debe estar habilitada en la configuración del dispositivo o se debe estar usando un servidor push o una puerta de enlace de conexión. Si no se cumplen estas condiciones, no podrá realizar la descarga.

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 desee descargar un archivo de seguimiento.

4. En la sección **Seguimiento**, haga clic en el botón **Archivos de seguimiento**.

   Se abre la ventana **Registros de seguimiento del dispositivo**, en la que se muestra una lista de archivos de seguimiento.

5. En la lista de archivos de seguimiento, seleccione el archivo que desee descargar.

6. Realice una de las siguientes acciones:

   - Si desea descargar el archivo seleccionado, haga clic en **Descargar**. Puede seleccionar uno o varios archivos para descargar.

   - Si desea descargar una parte del archivo seleccionado, haga lo siguiente:

     a. Haga clic en **Descargar una parte**.

        No puede descargar partes de varios archivos al mismo tiempo. Si selecciona más de un archivo de seguimiento, se deshabilita el botón **Descargar una parte**.

     b. En la ventana que se abre, indique el nombre y la parte del archivo que desee descargar.

        Para dispositivos basados en Linux, no está disponible la edición del nombre de la parte del archivo.

     c. Haga clic en **Descargar.**

El archivo seleccionado, o la parte seleccionada, se descargará en la ubicación que especifique.

Eliminar archivos de seguimiento

Puede eliminar los archivos de seguimiento que ya no necesite.

Para eliminar un archivo de seguimiento:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.

2. En la ventana de diagnóstico remoto que se abre, seleccione la pestaña **Registros de eventos**.

3. En la sección **Archivos de seguimiento**, haga clic en **Registros de Windows Update** o en **Registros de instalación remota**, dependiendo de cuáles sean los archivos de seguimiento que desee eliminar.

   Se abre la ventana **Registros de seguimiento del dispositivo**, en la que se muestra una lista de archivos de seguimiento.

4. En la lista de archivos de seguimiento, seleccione uno o varios archivos que desee eliminar.

5. Haga clic en el botón **Eliminar**.

Los archivo de seguimiento seleccionados se eliminan.

Descargar la configuración de las aplicaciones

Para poder descargar la configuración de la aplicación de un dispositivo cliente, se debe cumplir alguna de estas condiciones: la opción **No desconectar del Servidor de administración** debe estar habilitada en la configuración del dispositivo o se debe estar usando un servidor push o una puerta de enlace de conexión. Si no se cumplen estas condiciones, no podrá realizar la descarga.

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 las aplicaciones**, haga clic en el botón **Descargar** para descargar la información sobre la configuración de las aplicaciones instaladas en el dispositivo cliente.

En la ubicación especificada, se descarga el archivo ZIP con la información.

Descargar información del sistema desde un dispositivo cliente

Para poder descargar la información del sistema en su dispositivo de un dispositivo cliente, se debe cumplir alguna de estas condiciones: la opción **No desconectar del Servidor de administración** debe estar habilitada en la configuración del dispositivo o se debe estar usando un servidor push o una puerta de enlace de conexión. Si no se cumplen estas condiciones, no podrá realizar la descarga.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

Para descargar la información del sistema de un dispositivo cliente, siga los siguientes pasos:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Información del sistema**.
3. Haga clic en el botón **Descargar** para descargar la información del sistema sobre el dispositivo cliente.

En la ubicación especificada, se descarga el archivo con la información.

Descargar registros de eventos

Para poder descargar los registros de eventos de un dispositivo cliente, se debe cumplir alguna de estas condiciones: la opción **No desconectar del Servidor de administración** debe estar habilitada en la configuración del dispositivo o se debe estar usando un servidor push o una puerta de enlace de conexión. Si no se cumplen estas condiciones, no podrá realizar la descarga.

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 que desee descargar.
4. Realice una de las siguientes acciones:
   - Si desea descargar el archivo de registro seleccionado, haga clic en **Descargar archivo completo**.

- Si desea descargar una parte del archivo de registro seleccionado, haga lo siguiente:

  a. Haga clic en **Descargar una parte**.

  No puede descargar partes de varios registros al mismo tiempo. Si selecciona más de un registro de eventos, se deshabilita el botón **Descargar una parte**.

  b. En la ventana que se abre, indique el nombre y la parte del registro que desee descargar.

  c. Haga clic en **Descargar**.

El registro de eventos seleccionado, o la parte seleccionada, se descarga en la ubicación especificada.

Iniciar, detener o reiniciar la aplicación

Puede iniciar, detener y reiniciar las aplicaciones instaladas en los dispositivos cliente.

Para iniciar, detener o reiniciar una aplicación:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
3. En la lista de aplicaciones, seleccione la aplicación que desee iniciar, detener o reiniciar.
4. Haga clic en uno de los siguientes botones para realizar la acción correspondiente:

   - **Detener la aplicación**

     Este botón solo estará disponible si la aplicación se encuentra en ejecución.

   - **Reiniciar aplicación**

     Este botón solo estará disponible si la aplicación se encuentra en ejecución.

   - **Iniciar la aplicación**

     Este botón solo estará disponible si la aplicación no se encuentra en ejecución.

   Dependiendo de la acción que haya elegido, la aplicación seleccionada se iniciará, se detendrá o se reiniciará en el dispositivo cliente.

Si elige reiniciar el Agente de red, se le advertirá que la conexión entre el dispositivo y el Servidor de administración se cerrará.

Realizar un diagnóstico remoto 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 diagnóstico**.

   Se iniciará el proceso de diagnóstico remoto y se generará un informe con el resultado. Cuando se complete el proceso, la aplicación le permitirá hacer clic en el botón **Descargar informe de diagnóstico**.

5. Haga clic en el botón **Descargar informe de diagnóstico** para descargar el informe.

En la ubicación especificada, se descarga el archivo.

Ejecutar una aplicación en un dispositivo cliente

Ocasionalmente, 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:

  ```
  echo some result > $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**, seleccione el tipo de objeto que desea cargar:

   - Seleccione **Archivo** para cargar el archivo ejecutable.

   - Seleccione **Carpeta** para cargar la carpeta que contiene la aplicación que desea ejecutar en el dispositivo cliente.

     Si selecciona 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.

   - Seleccione **Archivo comprimido** para cargar el archivo ZIP que contiene la aplicación que desea ejecutar en el dispositivo cliente.

     Si selecciona 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 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 ejecuta en un dispositivo remoto.

4. Para cargar el objeto, selecciónelo en la ventana del sistema o arrástrelo al campo de carga.
5. Si es necesario, en el campo **Argumentos para 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 seleccionada en un dispositivo cliente.
7. Una vez completada con éxito la ejecución de la aplicación, descargue los resultados 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 completó el diagnóstico remoto del dispositivo cliente mediante la aplicación.

Crear un archivo de volcado para una aplicación

El archivo de volcado de una aplicación le permite ver los parámetros de la aplicación que se ejecuta en un dispositivo cliente en un momento determinado. Este archivo también contiene información sobre los módulos que se cargaron para una aplicación.

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 característica no es compatible.

Si desea crear un archivo de volcado para una aplicación:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, haga clic en la pestaña **Ejecución de una aplicación remota**.
3. En la sección **Generación de un volcado de memoria del proceso**, especifique el archivo ejecutable de la aplicación para la que desea generar un archivo de volcado.
4. Haga clic en el botón **Descargar** para guardar el archivo de volcado para la aplicación especificada.

   Si la aplicación especificada no se está ejecutando en el dispositivo cliente, se muestra el mensaje de error.

Conexión remota al escritorio de un dispositivo cliente

Puede obtener acceso remoto al escritorio de un dispositivo cliente a través del Agente de red instalado en ese dispositivo. El Agente de red permite conectarse incluso si el dispositivo cliente tiene cerrados los puertos TCP y UDP.

Tras conectarse a un dispositivo, tendrá acceso completo a la información que contenga y podrá administrar las aplicaciones instaladas en él.

Las conexiones remotas deben estar permitidas por el sistema operativo del dispositivo administrado al que pretenda acceder. En Windows 10, por ejemplo, debe estar habilitada la opción **Permitir conexiones de Asistencia remota a este equipo**, que se encuentra en **Panel de control → Sistema y seguridad → Sistema → Configuración de Acceso remoto**. Si tiene una licencia para la característica Administración de vulnerabilidades y parches, puede habilitar esta opción por la fuerza al conectarse al dispositivo administrado. Si no tiene una licencia para esta función, habilite la opción de manera local en el dispositivo administrado. No podrá establecer una conexión remota si esta opción está deshabilitada.

Para conectarse a un dispositivo remoto, debe contar con dos utilidades:

- La utilidad klsctunnel, desarrollada por Kaspersky. Este programa debe estar almacenado en 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 que la Consola de administración se conecte a un puerto TCP específico de un dispositivo administrado a través de un túnel que se hace pasar por el Servidor de administración y luego por el Agente de red. 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 conecte a la sesión, el sistema desconectará al usuario original sin previo aviso.

Para que pueda conectarse al escritorio de un dispositivo cliente, se deben cumplir 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.

  El número total máximo 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 escritorio remoto**.

   Se abre la ventana Conectar con 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 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. Ingrese las credenciales de la cuenta con la que haya iniciado sesión 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 a través del Agente de red instalado en ese 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 sin desconectar a la persona que la inició. En tal caso, compartirá el acceso al escritorio con el usuario de la sesión.

Para conectarse a un dispositivo remoto, debe contar con dos utilidades:

- La utilidad klsctunnel, desarrollada por Kaspersky. Este programa debe estar almacenado en 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 que la Consola de administración se conecte a un puerto TCP específico de un dispositivo administrado a través de un túnel que se hace pasar por el Servidor de administración y luego por el Agente de red. 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. Cuando se conecte a una sesión existente del escritorio remoto, el usuario que haya iniciado esa sesión en el dispositivo verá una solicitud de conexión. No se guardará ningún tipo de información sobre las actividades que se realicen de manera remota en el dispositivo, ni sobre los resultados de esas actividades, en los informes generados por Kaspersky Security Center Cloud Console.

  Si lo desea, puede auditar las actividades que realizan los usuarios en los dispositivos cliente remotos. Cuando la función de auditoría está activada, la aplicación guarda información sobre los archivos que el administrador abre o modifica en el dispositivo cliente.

Para que pueda conectarse al escritorio de un dispositivo cliente a través de Windows Desktop Sharing, se deben cumplir las siguientes condiciones:

- Su estación de trabajo debe tener Microsoft Windows Vista o una versión de Windows posterior.

  Para determinar si la característica Windows Desktop Sharing está disponible en su edición de Windows, verifique que el CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} exista 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 debe usar una licencia de 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 el número total máximo 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 Windows Desktop Sharing:

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 **Windows Desktop Sharing**.

   Se abre el asistente de Windows Desktop Sharing.

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.

   Una vez que el usuario autoriza la sesión de escritorio compartido, 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. Cuando funcionan en modo Aprendizaje inteligente, las reglas detectan comportamientos anómalos y envían informes sobre cada detección 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 si las detecciones son válidas o agregarlas como exclusiones para que el tipo de comportamiento deje de considerarse anómalo.

La información sobre las detecciones se almacena en el registro de eventos del Servidor de administración (junto con otros eventos) y en el informe del Control de anomalías adaptativo.

Para obtener más información acerca del Control de anomalías adaptativo y sus reglas, 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, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del objeto de origen**

Hash SHA256 del archivo de origen (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del proceso de destino**

  Ruta al proceso de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del proceso de destino**

  Hash SHA256 del archivo de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del objeto de destino**

  Ruta al objeto de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del objeto de destino**

  Hash SHA256 del archivo de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

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 le interese.
4. Haga click en el enlace **Propiedades**.

   Se abrirá la ventana de propiedades del objeto, en la que encontrará información sobre el elemento que haya 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 se sumará 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 iniciará el Asistente para agregar exclusiones. Siga las instrucciones del asistente.

Si rechaza o confirma un elemento, se lo excluirá de la lista de detecciones la siguiente vez que el dispositivo cliente se sincronice con el Servidor de administración. El elemento dejará de aparecer en la lista.

Adición de exclusiones para las reglas del Control de anomalías adaptativo

El Asistente para agregar exclusiones permite incorporar exclusiones para las reglas del Control de anomalías adaptativo para Kaspersky Endpoint Security para Windows.

Para iniciar el Asistente para agregar 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 se abre, seleccione uno o más elementos de la lista de detecciones y, a continuación, 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 iniciará el Asistente para agregar exclusiones. Avance por el asistente utilizando el botón **Siguiente**.

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

En un primer momento, la jerarquía de grupos de administración contiene solo un grupo de administración llamado **Dispositivos administrados**. Puede agregar 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 en el que desea incluir el nuevo grupo de administración.
3. Haga clic en el botón **Agregar**.
4. En la ventana que se abre, escriba un nombre para el grupo y haga clic en **Agregar**.

   En la jerarquía de grupos de administración, aparecerá un nuevo grupo de administración con el nombre que haya indicado.

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 ofrece una única directiva para cada aplicación de Kaspersky disponible en un grupo de administración. Una directiva tiene uno de los siguientes estados (consulte la tabla a continuación):

Estado de la directiva

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

Las directivas funcionan de acuerdo con las siguientes reglas:

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

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

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

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

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

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

No es posible crear una directiva para el 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*.
Imponer	Cuando un ajuste tiene un candado cerrado a su lado y el interruptor de bloqueo está activado, el valor definido para ese ajuste es el que se aplica en los dispositivos sujetos a la directiva. El usuario no puede modificar el valor del ajuste mediante la interfaz de la aplicación administrada. Estos ajustes se consideran *bloqueados*.

Recomendamos encarecidamente que cierre los bloqueos para la configuración de la directiva que desea aplicar en los dispositivos administrados. La configuración de la directiva desbloqueada se puede reasignar mediante la configuración de la aplicación Kaspersky en un dispositivo administrado.

Puede utilizar el interruptor de bloqueo para lo siguiente:

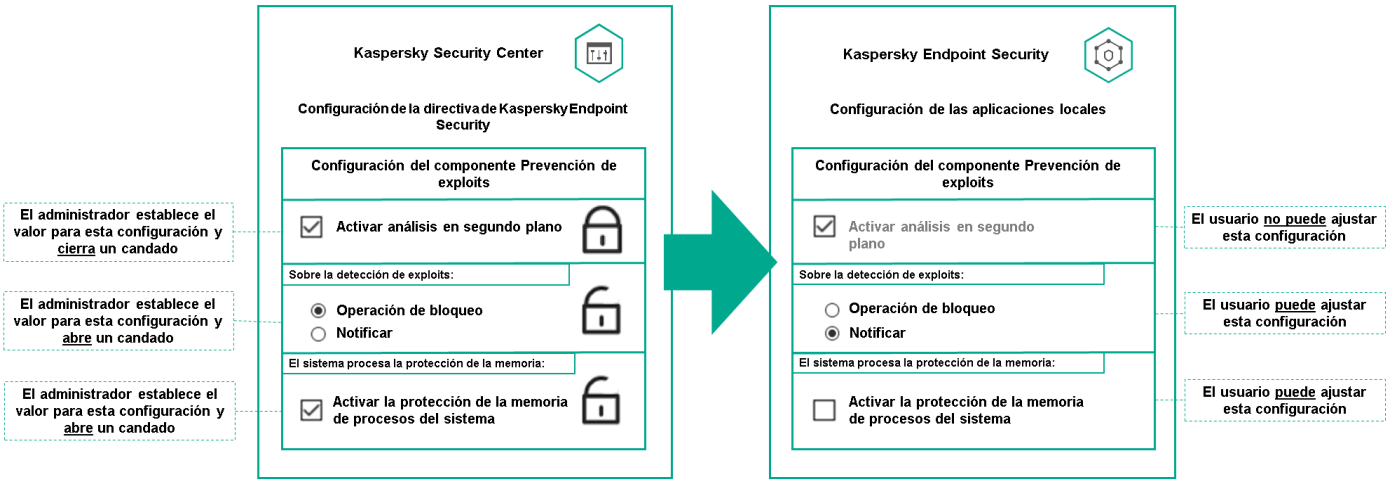
- Bloquear ajustes en la directiva de un subgrupo de administración
- Bloquear los ajustes de una aplicación de Kaspersky instalada en un dispositivo administrado

De este modo, un ajuste bloqueado se utiliza para formar y aplicar los ajustes vigentes de un dispositivo administrado.

El proceso para formar y aplicar los ajustes vigentes consta de las siguientes acciones:

- El dispositivo administrado aplica los valores de configuración definidos localmente en la aplicación de Kaspersky.
- El dispositivo administrado aplica los valores de configuración que se encuentran bloqueados en la directiva.

La directiva contiene los mismos ajustes que la aplicación de Kaspersky administrada. Cuando se modifican los ajustes dentro de una directiva, se modifican los ajustes en la aplicación de Kaspersky instalada en el dispositivo administrado. Los ajustes bloqueados no se pueden modificar en el dispositivo administrado (vea la siguiente imagen):



Candados y configuración de una aplicación de Kaspersky

Herencia en las directivas y los perfiles de directivas

En esta sección, se brinda información sobre la jerarquía y la herencia en el ámbito de las directivas y los perfiles de directivas.

Jerarquía de directivas

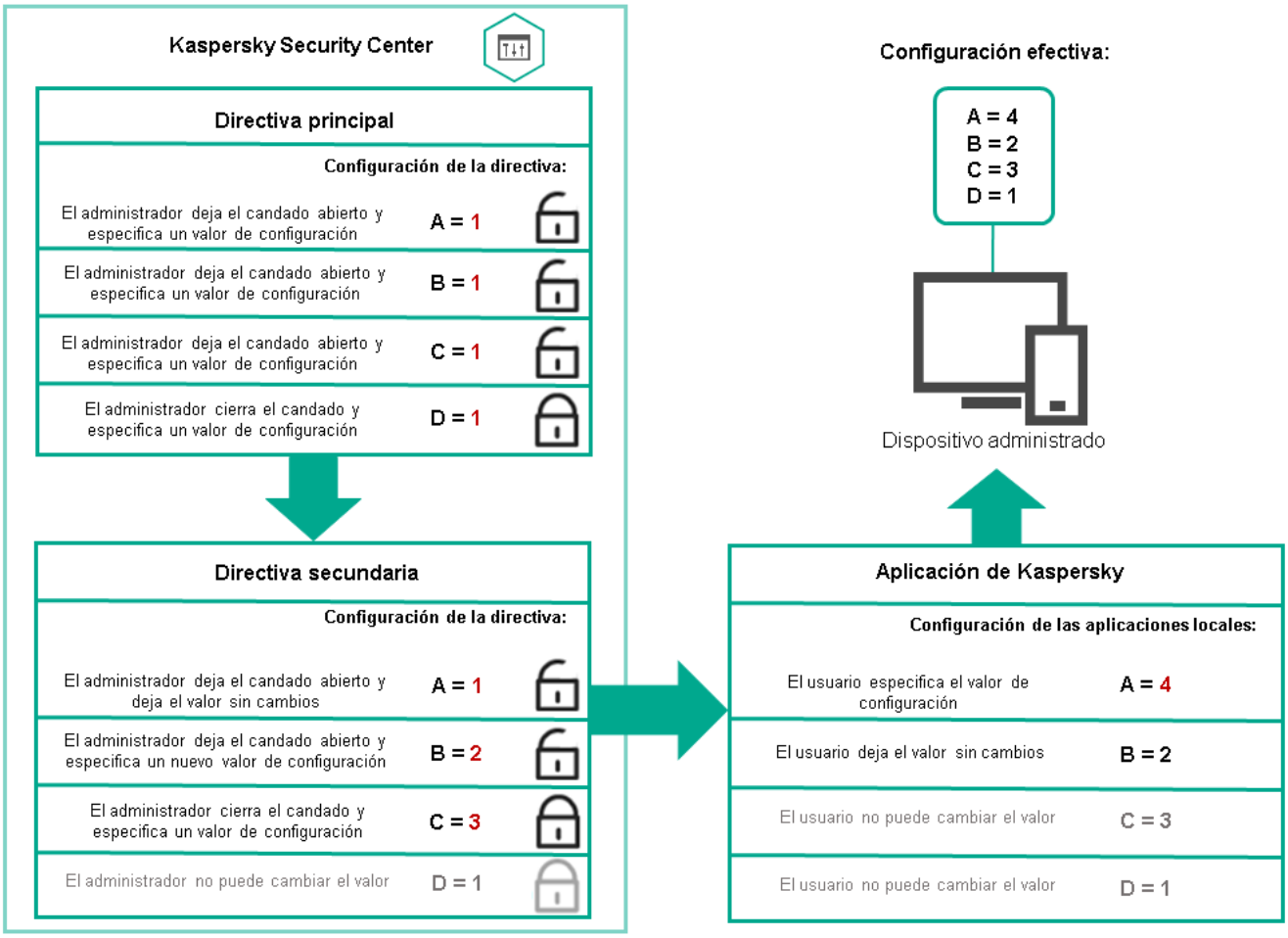
Si distintos dispositivos necesitan diferentes configuraciones, puede organizar los dispositivos en grupos de administración.

Puede especificar una directiva para un solo grupo de administración. La configuración de la directiva se puede *heredar*. La herencia hace que un subgrupo o grupo secundario de un grupo primario (un grupo de administración ubicado en un nivel superior) reciba valores de configuración de una directiva definida para ese grupo primario.

En lo sucesivo, se usará el término *directiva primaria* para hacer referencia a una directiva definida para un grupo primario. Una directiva para un subgrupo o grupo secundario se denominará *directiva secundaria*.

De forma predeterminada, existe al menos un grupo de dispositivos administrados en el Servidor de administración. Si crea grupos personalizados, se los creará como subgrupos o grupos secundarios de este grupo de dispositivos administrados.

Las directivas de una misma aplicación se afectan las unas a las otras siguiendo el orden jerárquico de los grupos de administración. Los ajustes que se bloquean en una directiva de un grupo de administración primario (de nivel superior) sobrescriben los valores de configuración en la directiva de un subgrupo (vea la siguiente imagen).

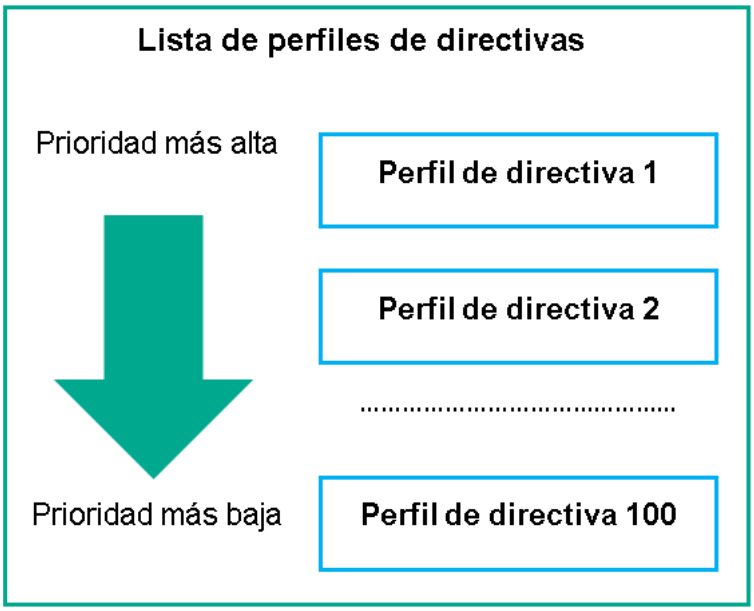


Jerarquía de directivas

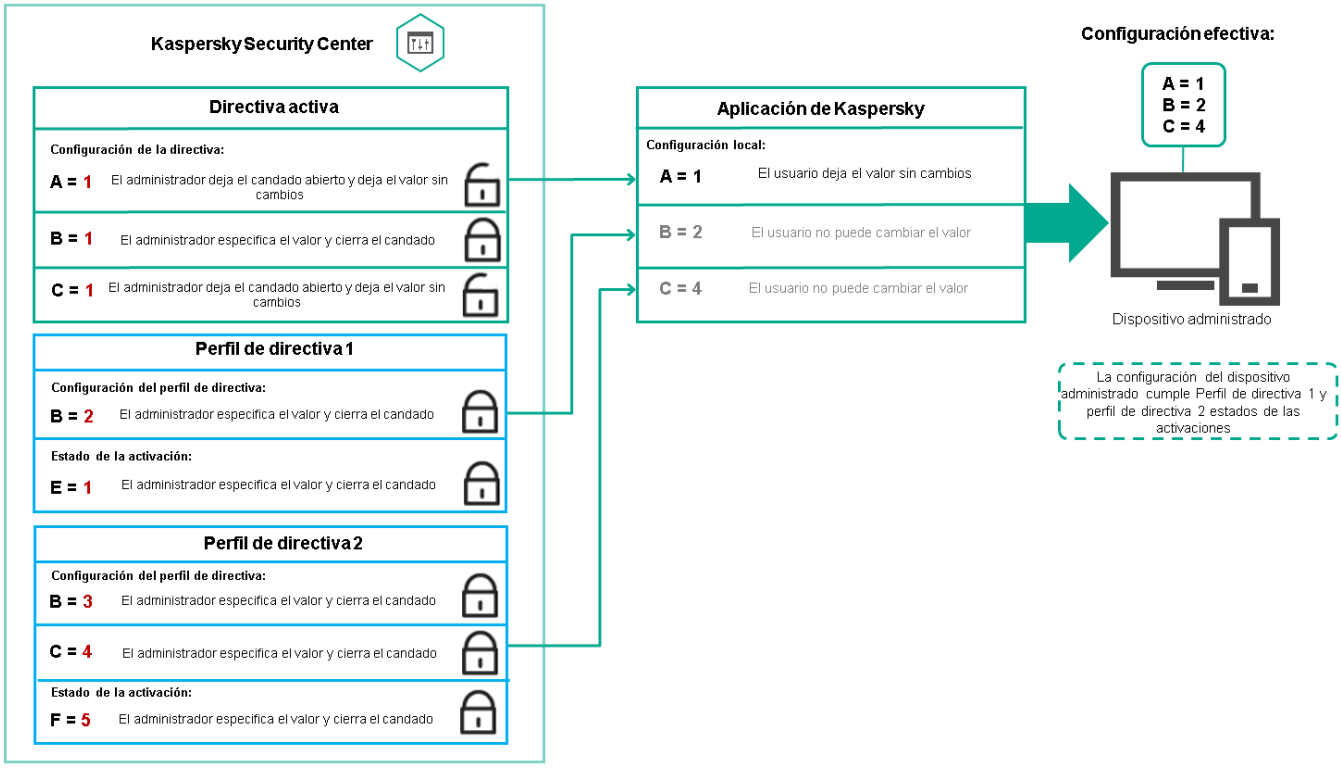
Perfiles de directivas en una jerarquía de directivas

Los perfiles de directivas tienen las siguientes condiciones de asignación de prioridad:

- La posición de un perfil en una lista de perfiles indica su prioridad. La prioridad de un perfil puede modificarse. La posición más alta en la lista representa la prioridad más alta (vea la siguiente imagen).



- 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).



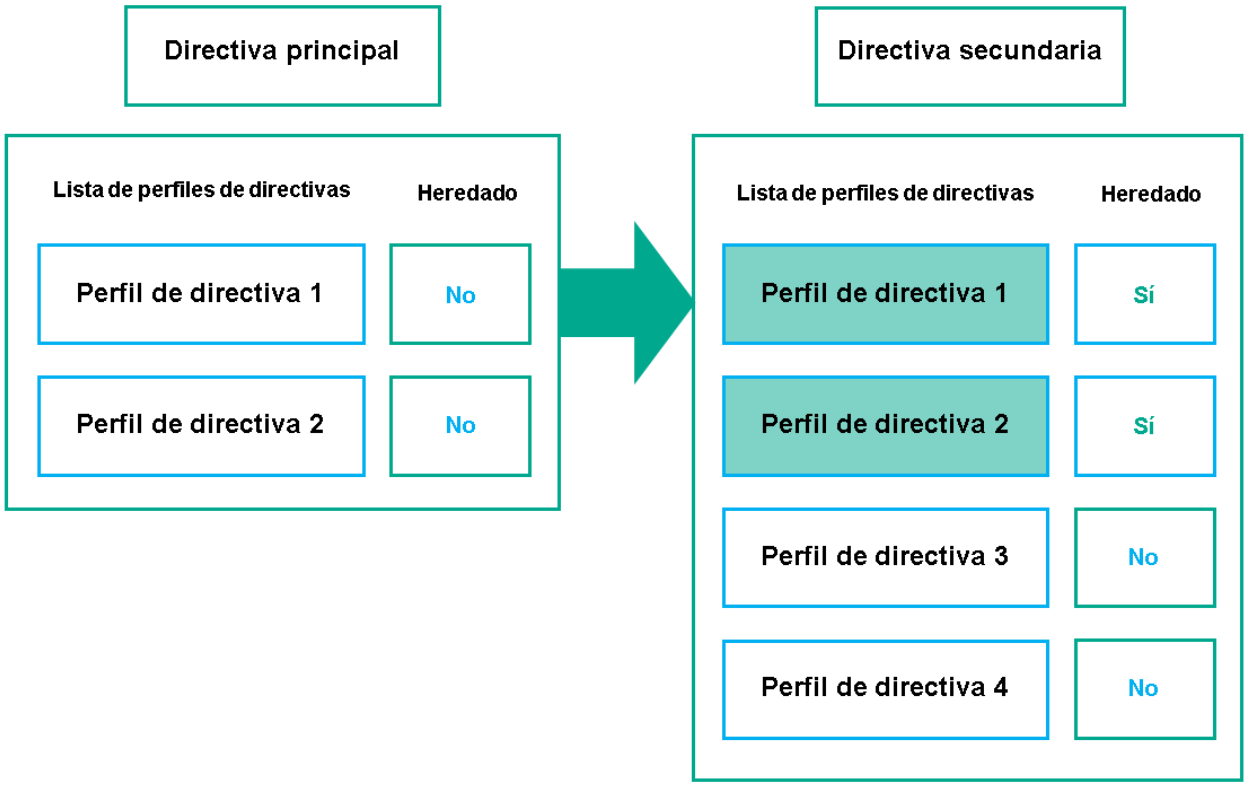
La configuración del dispositivo administrado cumple las condiciones de activación de varios perfiles de directiva

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).

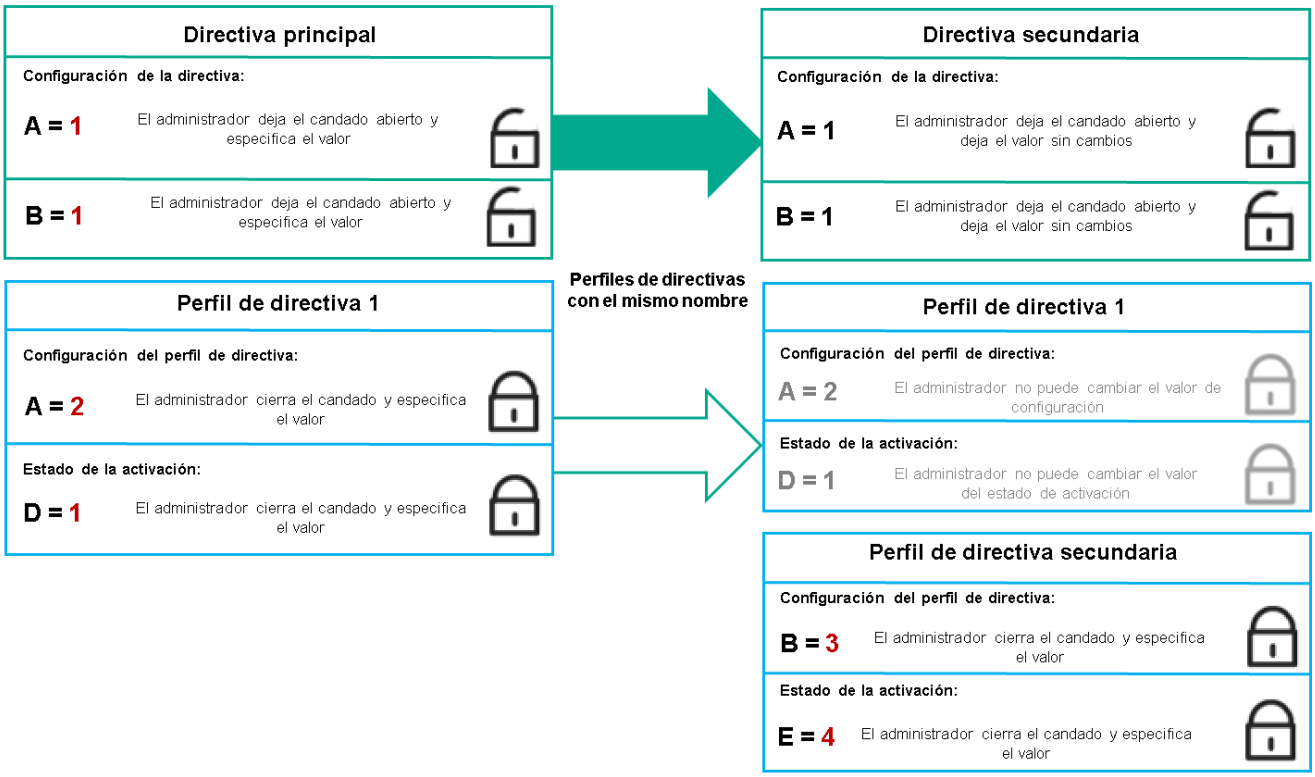


Herencia de perfiles de directivas

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 es posible crear una directiva para el Servidor de administración.

Para crear una directiva:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en **Agregar**.

   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 una categoría de su interés. En el panel de resultados de la derecha, modifique la configuración de la directiva. Puede editar los ajustes de configuración disponibles en cada categoría (sección).

   Los ajustes de configuración disponibles dependen de la aplicación a la que corresponde la 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 revisiones**.

Ajustes generales de una directiva

General

Utilice la pestaña **General** para modificar el estado de la directiva y configurar los ajustes que controlan la herencia de sus valores de configuración:

- 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 primaria

    Si habilita esta opción, la directiva heredará los valores de configuración definidos en la directiva del grupo de nivel superior. Estos valores, en consecuencia, estarán bloqueados.

    Esta opción está activada de forma predeterminada.

  - Forzar la herencia de configuración en las directivas secundarias

    Si habilita esta opción, cuando modifique la directiva y se apliquen los cambios, ocurrirá lo siguiente:
    - Los valores de configuración de la directiva se propagarán a las directivas de los subgrupos de administración (es decir, a las directivas secundarias).
    - En la ventana de propiedades de cada directiva secundaria, dentro del bloque **Herencia de configuración** de la sección **General**, se habilitará automáticamente la opción **Heredar configuración de la directiva primaria**.

    Habilitar esta opción hace que los ajustes de las directivas secundarias se bloqueen.

    Esta opción está deshabilitada de forma predeterminada.

Configuración de eventos

En la pestaña **Configuración de eventos**, puede configurar ajustes relativos al registro de los eventos y a las notificaciones que se envían cuando ocurre un evento. Los eventos están distribuidos por nivel de importancia en las siguientes pestañas:

- **Crítico**

  La sección **Crítico** no se muestra en las propiedades de la directiva del Agente de red.

- **error funcional**
- **Advertencia**
- **Información**

Cada sección contiene una lista con los distintos tipos de eventos y la cantidad de días por las que cada evento se deja almacenado, de manera predeterminada, en el Servidor de administración. Haga clic en un tipo de evento para configurar los siguientes ajustes:

- **Registro de los eventos**

  Puede especificar cuántos días se conservará el evento y dónde se lo guardará:

  - **Guardar en la base de datos del Servidor de administración por (días)**
  - **Guardar en el registro de eventos del SO del dispositivo**

- **Notificaciones sobre los eventos**

  Puede indicar si desea recibir una notificación 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 desea cambiar estos ajustes, puede hacerlo en la pestaña **Correo electrónico**.

Además, la pestaña **Configuración de eventos** muestra una notificación cuando se agregan 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 revisiones

La pestaña **Historial de revisiones** permite ver la lista de revisiones de la directiva y, de ser necesario, revertir los cambios realizados en ella.

Habilitar y deshabilitar una opción de herencia en las directivas

Para habilitar o deshabilitar la opción de herencia en una directiva:

1. Abra la directiva que tenga en mente.
2. Abra la pestaña **General**.
3. Habilite o deshabilite la herencia en la directiva:
   - Si habilita la opción **Heredar configuración de la directiva primaria** en una directiva secundaria y un administrador bloquea algunos ajustes de configuración en la directiva primaria, no podrá cambiar esos ajustes en la directiva secundaria.
   - Si deshabilita la opción **Heredar configuración de la directiva primaria** en una directiva secundaria, podrá cambiar todos los ajustes de la directiva secundaria aunque haya ajustes bloqueados en la directiva primaria.
   - Si habilita la opción **Forzar la herencia de configuración en las directivas secundarias** en el grupo primario, se habilitará la opción **Heredar configuración de la directiva primaria** en cada directiva secundaria. No podrá deshabilitar esta opción en ninguna directiva secundaria. Los grupos secundarios heredarán por la fuerza todos los ajustes que se bloqueen en la directiva primaria; los valores de estos ajustes no se podrán modificar en los grupos secundarios.
4. Haga clic en el botón **Guardar** para guardar los cambios o haga clic en el botón **Cancelar** para rechazar los cambios.

De manera predeterminada, la opción **Heredar configuración de la directiva primaria** está habilitada en las directivas nuevas.

Si una directiva tiene perfiles, todas las directivas secundarias los heredan.

Copiar una directiva

Puede copiar directivas de un grupo de administración a otro.

Para copiar una directiva a otro grupo de administración:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Marque la casilla ubicada junto a la directiva (o las directivas) que desee copiar.
3. Haga clic en el botón **Copiar**.

   En el lado derecho de la pantalla, verá el árbol con los grupos de administración.
4. En el árbol, seleccione el grupo de destino (es decir, el grupo al que desee copiar la directiva o las directivas).
5. Haga clic en el botón **Copiar** que está al final de la pantalla.
6. Haga clic en **Aceptar** para confirmar la operación.

Las directivas que haya seleccionado se copiarán al grupo de destino con todos sus perfiles. El estado de estas directivas en el grupo de destino será **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

Si el grupo de destino contiene una directiva con el mismo nombre que la que se quiere mover, se agregará un índice secuencial —en formato (<siguiente número en la serie>), por ejemplo, (1)— al nombre de la directiva trasladada.

Mover una directiva

Puede mover directivas de un grupo de administración a otro. Esto puede ser útil si necesita eliminar un grupo, por ejemplo, pero quiere utilizar sus directivas para un grupo diferente. En tal caso, antes de eliminar el grupo que ya no necesita, puede mover sus directivas al nuevo grupo.

Para mover una directiva a otro grupo de administración:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Marque la casilla ubicada junto a la directiva (o las directivas) que desee mover.
3. Haga clic en el botón **Mover**.

   En el lado derecho de la pantalla, verá el árbol con los grupos de administración.
4. En el árbol, seleccione el grupo de destino (es decir, el grupo al que desee mover la directiva o las directivas).
5. Haga clic en el botón **Mover** en la parte inferior de la pantalla.
6. Haga clic en **Aceptar** para confirmar la operación.

Si la directiva del grupo de origen no es una directiva heredada, se la moverá al grupo de destino junto con todos sus perfiles. El estado de la directiva en el grupo de destino será **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

Si la directiva del grupo de origen es una directiva heredada, permanecerá en el grupo de origen. En lugar de moverla, se la copiará al grupo de destino junto con todos sus perfiles. El estado de la directiva en el grupo de destino será **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

Si el grupo de destino contiene una directiva con el mismo nombre que la que se quiere mover, se agregará un índice secuencial —en formato (<siguiente número en la serie>), por ejemplo, (1)— al nombre de la directiva trasladada.

Exportación de una directiva

Kaspersky Security Center Cloud Console permite guardar una directiva, su configuración y sus perfiles en un archivo KLP. El archivo KLP puede usarse para importar la directiva guardada en Kaspersky Security Center Windows o Kaspersky Security Center Linux.

Para exportar una directiva:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Marque la casilla ubicada junto a la directiva que desee exportar.

   No es posible exportar más de una directiva a la vez. Si selecciona más de una directiva, el botón **Exportar** se desactivará.
3. Haga clic en el botón **Exportar**.
4. En la ventana **Guardar como** que se abrirá, ingrese la ruta y el nombre del archivo en el que se guardará la directiva. Haga clic en el botón **Guardar**.

   La ventana **Guardar como** aparecerá solo si utiliza los navegadores Google Chrome, Microsoft Edge u Opera. Si utiliza otro navegador, el archivo de la directiva se guardará automáticamente en la carpeta **Descargas**.

Importación de una directiva

Kaspersky Security Center Cloud Console permite importar una directiva guardada en un archivo KLP. El archivo KLP contiene la directiva exportada, su configuración y sus perfiles.

Para importar una directiva:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.
2. Haga clic en el botón **Importar**.
3. Haga clic en el botón **Examinar** para elegir el archivo de política que desee importar.
4. En la ventana que se abrirá, ingrese la ruta al archivo KLP de la directiva y haga clic en el botón **Abrir**. Tenga en cuenta que no podrá seleccionar más de un archivo de directiva.

   Comenzará a procesarse la directiva.
5. Una vez que la directiva se haya procesado, seleccione el grupo de administración al que desee aplicarla.
6. Haga clic en el botón **Completado** para finalizar la importación de políticas.

Aparecerá una notificación con los resultados de la importación. Si la tarea se importa correctamente, puede hacer clic en el vínculo **Detalles** para ver las propiedades de la misma.

Una vez que se complete la importación, la directiva aparecerá en la lista de directivas. También se importarán la configuración y los perfiles de la directiva. La directiva importada tendrá estado inactivo independientemente del estado que se haya seleccionado al exportarla. Puede cambiar el estado en las propiedades de la directiva.

Si la directiva importada tiene el mismo nombre que una directiva existente, el nombre de la directiva importada se complementará con un índice secuencial en formato **(<siguiente número secuencial>)**, por ejemplo **(1)** o **(2)**.

Ver el gráfico de distribución de una directiva

Kaspersky Security Center Cloud Console permite ver el estado de aplicación de una directiva en cada dispositivo a través de un gráfico que representa el estado de distribución de la directiva.

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 vínculo **Distribución**.

   Se abre la ventana **<Nombre de la directiva>: resultados de la distribución**.
4. En la ventana **<Nombre de la directiva>: resultados de la distribución**, encontrará la **Descripción del estado (si está disponible)** de la directiva.

Puede cambiar la cantidad de resultados que aparecen en la lista que detalla la distribución de la directiva. El número máximo de dispositivos es 100 000.

Para cambiar la cantidad de dispositivos que se muestran en la lista con los resultados de la distribución de una directiva:

1. En el menú principal, vaya a la configuración de su cuenta y, a continuación, seleccione **Opciones de interfaz.**
2. En **Límite de dispositivos que se incluirán en los resultados de distribución de las directivas**, ingrese el número de dispositivos (hasta 100 000).

   De manera predeterminada, el límite es de 5000.
3. Haga clic en **Guardar**.

El cambio se aplica y se guarda.

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 icono 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 las directivas que se activarán ante un 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 **Agregar**.

   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, marque 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

En Kaspersky Security Center Cloud Console, el estado, la configuración, las directivas y las tareas de los dispositivos administrados se sincronizan en forma automática. No obstante, en algunos casos se necesita tener la certeza de que la sincronización con un dispositivo puntual se ha realizado.

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, luego, seleccione el grupo de administración que contenga los dispositivos para 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

A veces, tras modificar la directiva de una aplicación de Kaspersky en el Servidor de administración, resulta de interés verificar que la misma se haya entregado a un dispositivo en particular. 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 **Agregar**.

3. Si lo desea, cambie el nombre predeterminado y las opciones de directiva predeterminadas del perfil.

4. Seleccione la pestaña **Configuración de la aplicación**.

   O, si lo prefiere, puede hacer clic en **Guardar** y salir. El perfil que creó aparece en la lista de perfiles de directivas y podrá editar su configuración más adelante.

5. En la pestaña **Configuración de la aplicación**, en el panel izquierdo, seleccione la categoría que desea y, en el panel de resultados de la derecha, edite la configuración del perfil. Puede editar los ajustes disponibles en cada categoría (sección) para el perfil de directiva.

   Al editar la configuración, puede hacer clic en **Cancelar** para cancelar la última operación.

6. Haga clic en **Guardar** para guardar el perfil.

El perfil aparecerá en la lista de perfiles de directiva.

Modificar un perfil de directiva

La posibilidad de modificar un perfil de directiva solo está disponible para las directivas de Kaspersky Endpoint Security para Windows.

Para modificar un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.

2. En la pestaña **Perfiles de directiva**, seleccione el perfil de directiva que desee modificar.

   Se abre la ventana de propiedades del perfil de directiva.

3. En la ventana de propiedades, configure el perfil:

   - De ser necesario, en la pestaña **General**, habilite o deshabilite el perfil y cámbiele el nombre.
   - Modifique las reglas de activación del perfil.

- Modifique los ajustes de la aplicación.

Para obtener detalles sobre los ajustes de las aplicaciones de seguridad, consulte la documentación de esas aplicaciones.

4. Haga clic en **Guardar**.

Los cambios de configuración entrarán en vigor cuando el dispositivo se sincronice con el Servidor de administración (si el perfil de directiva está activo) o cuando se accione una de las reglas de activación (si el perfil de directiva está inactivo).

Copiar un perfil de directiva

Puede copiar un perfil de directiva a la directiva actual o a otra si, por ejemplo, quiere tener perfiles idénticos para directivas diferentes. También puede copiar un perfil si necesita tener dos o más perfiles que se diferencien solo en un pequeño número de ajustes.

Para copiar un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva. Si la directiva no tiene perfiles, verá una tabla vacía.

2. En la pestaña **Perfiles de directiva**, seleccione el perfil de directiva que desee copiar.

3. Haga clic en **Copiar**.

4. En la ventana que se abre, seleccione la directiva a la que desee copiar el perfil.

   Puede copiar un perfil de directiva en la misma directiva o en una directiva que especifique.

5. Haga clic en **Copiar**.

El perfil de directiva se copia a la directiva seleccionada. La copia del perfil obtiene la prioridad más baja. Cuando un perfil se copia a su misma directiva de origen, se agrega un índice numérico entre paréntesis al nombre de la copia (por ejemplo: (1), (2), etc.).

Más adelante, podrá cambiar la configuración del perfil, incluyendo su nombre y su prioridad; el perfil de directiva original no sufrirá modificaciones.

Crear una regla de activación para un perfil de directiva

Para crear una regla de activación para un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.

2. En la pestaña **Perfiles de directiva**, haga clic en el perfil de directiva para el que desee crear la regla de activación.

   Si la lista de perfiles de la directiva está vacía, puede crear un perfil de directiva.

3. En la pestaña **Reglas de activación**, haga clic en el botón **Agregar**.

   Se abre la ventana con las reglas de activación del perfil de directiva.

4. Escriba un nombre para la regla.

5. Active las casillas de verificación ubicadas junto a las condiciones que afectarán la activación del nuevo perfil de directiva:

   - Reglas generales para la activación del perfil de directiva

     Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo dependiendo del estado del modo sin conexión de ese dispositivo, de las reglas de conexión con el Servidor de administración o de las etiquetas que el dispositivo tenga asignadas.

     Si elige esta opción, defina esto en el paso siguiente:

     - Estado del dispositivo

       Define la condición relativa a la presencia del dispositivo en la red:

       - **En línea**: el dispositivo está en la red, lo que significa que el Servidor de administración está disponible.
       - **Sin conexión**: el dispositivo está en una red externa, lo que significa que el Servidor de administración no está disponible.
       - **N/D**: no se aplica este criterio.

     - Una regla de conexión al Servidor de administración está activa en este dispositivo

       Elija la condición de activación del perfil de directiva (el hecho de que la regla se ejecute o no) y seleccione el nombre de la regla.

       La regla define la ubicación de red del dispositivo para la conexión con el Servidor de administración. Las condiciones de esta regla se deben cumplir (o no se deben cumplir) para que se active el perfil de directiva.

       Puede crear o configurar una descripción de ubicación de red de dispositivos para la conexión con un Servidor de administración en una regla de cambio de Agente de red.

   - **Reglas para un propietario del dispositivo específico**

     Si elige esta opción, defina esto en el paso siguiente:

     - Propietario del dispositivo

Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo dependiendo de quién sea el propietario del mismo. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:

- El dispositivo pertenece al propietario especificado (signo "=").
- El dispositivo no pertenece al propietario especificado (signo "≠").

  Tenga en cuenta que la lista de usuarios está filtrada 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 forma predeterminada.

- **El propietario del dispositivo está incluido en un grupo de seguridad interno**

  Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo dependiendo de si el propietario del mismo pertenece o no a un grupo de seguridad interno 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 está filtrada 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 especificar el nombre de 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 forma predeterminada.

- **Reglas para las especificaciones del hardware**

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo dependiendo de la cantidad de memoria y del número de procesadores lógicos que el dispositivo tenga.

  Si elige esta opción, defina esto en el paso siguiente:

  - **Tamaño de RAM, en MB**

    Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo en función de la cantidad de RAM que este posea. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:

    - El tamaño de la RAM del dispositivo está por debajo del valor especificado (signo "<").
    - El tamaño de la RAM del dispositivo está por encima del valor especificado (signo ">").

    Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá especificar la cantidad de RAM con la que deberá contar el dispositivo. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

- Número de procesadores lógicos

  Habilite esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo en función del número de procesadores lógicos que este tenga. En la lista desplegable bajo la casilla, seleccione el criterio que determinará la activación del perfil:

  - El número de procesadores lógicos del dispositivo es menor o igual que el valor especificado (signo "<").
  - El número de procesadores lógicos del dispositivo es mayor o igual que el valor especificado (signo ">").

  Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado. Podrá especificar la cantidad de procesadores lógicos con los que deberá contar el dispositivo. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

- **Reglas para la asignación de roles**

  Si elige esta opción, defina esto en el paso siguiente:

  Activar el perfil de directiva según el rol específico del propietario del dispositivo

  Seleccione esta opción para configurar y habilitar una regla que haga que el perfil se active en un dispositivo dependiendo del rol asignado al propietario del mismo. Utilice la lista de roles existentes para agregar el rol en forma manual.

  Si habilita esta opción, el perfil se activará en el dispositivo siguiendo el criterio configurado.

- Reglas para el uso de la etiqueta

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo dependiendo de las etiquetas asignadas al mismo. El perfil de directiva podrá activarse en dispositivos que tengan las etiquetas seleccionadas o que no tengan esas etiquetas.

  Si elige esta opción, defina esto en el paso siguiente:

  - Etiqueta

    En la lista de etiquetas, configure la regla que hará que los dispositivos que tengan ciertas etiquetas se incluyan en el perfil de directiva. Para configurar esta regla, active las casillas ubicadas junto a las etiquetas pertinentes.

    Si necesita agregar etiquetas nuevas, introdúzcalas en el campo que se encuentra sobre la lista y haga clic en el botón **Agregar**.

    El perfil de directiva incluirá aquellos dispositivos que, en su descripción, contengan todas las etiquetas seleccionadas. Si no activa estas casillas, no se aplicará este criterio. Estas casillas están desactivadas de manera predeterminada.

  - Aplicar a los dispositivos que no tengan las etiquetas especificadas

Habilite esta opción si tiene que invertir la selección de etiquetas.

Si habilita esta opción, el perfil de directiva incluirá aquellos dispositivos que no tengan, en su descripción, ninguna de las etiquetas seleccionadas. Si deshabilita esta opción, no se aplicará el criterio.

Esta opción está deshabilitada de forma predeterminada.

- **Reglas para el uso de Active Directory**

  Marque esta casilla para configurar reglas que hagan que el perfil de directiva se active en un dispositivo si el mismo pertenece a una unidad organizativa de Active Directory en particular o si el dispositivo o su propietario son miembros de un grupo de seguridad de Active Directory.

  Si elige esta opción, defina esto en el paso siguiente:

  - **Membrecía del propietario del dispositivo en un grupo de seguridad de Active Directory**

    Si habilita esta opción, el perfil de directiva se activará en un dispositivo si su propietario es miembro del grupo de seguridad especificado. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

  - **Membrecía del dispositivo en un grupo de seguridad de Active Directory**

    Si habilita esta opción, el perfil de directiva se activará en el dispositivo. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil. Esta opción está deshabilitada de forma predeterminada.

  - **Asignación de dispositivos en la unidad organizativa de Active Directory**

    Si habilita esta opción, el perfil de directiva se activará en un dispositivo si el mismo está incluido en la unidad organizativa de Active Directory especificada. Si no habilita esta opción, no se usará este criterio para regular la activación del perfil.

    Esta opción está deshabilitada de forma predeterminada.

El número de páginas adicionales del asistente dependerá de las opciones que haya elegido en el primer paso. Podrá modificar las reglas de activación del perfil de directiva más adelante.

6. Revise la lista de parámetros configurados. Si no hay errores en la lista, haga clic en **Crear**.

Se guardará el perfil. El perfil se activará en el dispositivo cuando se desencadenen las reglas de activación.

Las reglas de activación creadas para un perfil de directiva se muestran en las propiedades del perfil, dentro de la pestaña **Reglas de activación**. Puede modificar o eliminar cualquiera de las reglas de activación del perfil de directiva.

Existe la posibilidad de que varias reglas de activación se desencadenen simultáneamente.

Eliminar un perfil de directiva

Para eliminar un perfil de directiva:

1. Abra la lista de perfiles de la directiva pertinente.

   Se abre la lista de perfiles de la directiva.

2. En la pestaña **Perfiles de directiva**, marque la casilla ubicada junto al perfil de directiva que desee eliminar y haga clic en **Eliminar**.

3. En la ventana que se abre, haga clic de nuevo en **Eliminar**.

   El perfil de directiva se elimina. Si la directiva es heredada por un grupo de nivel inferior, el perfil permanece en ese grupo pero se convierte en el perfil de la directiva de ese grupo. De este modo, se evitan cambios radicales en la configuración de las aplicaciones administradas que se encuentran instaladas en los dispositivos de los grupos de nivel inferior.

Protección y cifrado de datos

El cifrado de datos reduce el riesgo de pérdida involuntaria de datos en caso de que le roben o pierda su computadora portátil o su disco duro, o en caso de que usuarios no autorizados y aplicaciones accedan a ellos.

Las siguientes aplicaciones de Kaspersky son compatibles con el cifrado de datos:

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

Puede modificar los ajustes de la interfaz de usuario para mostrar u ocultar algunos de los elementos de la interfaz que están vinculados a la función de administración del cifrado.

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.

Para configurar los ajustes de cifrado, deberá definir directivas de Kaspersky Endpoint Security para Windows a través de 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 para Mac

En dispositivos con macOS, puede utilizar el cifrado FileVault. Esta tecnología de cifrado puede habilitarse y deshabilitarse a través de Kaspersky Endpoint Security for Mac.

Para configurar los ajustes de cifrado, deberá definir directivas de Kaspersky Endpoint Security for Mac a través de Kaspersky Security Center 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** → **Unidades cifradas**.

Si la sección no aparece en el menú, significa que está oculta. En la configuración de la interfaz de usuario, habilite la opción **Mostrar protección y cifrado de datos** para mostrar la sección.

Puede exportar la lista de unidades cifradas a un archivo CSV o TXT. Para hacerlo, haga clic en el botón **Exportar a CSV** o **Exportar a TXT**.

Crear y ver informes de cifrado

Puede generar los siguientes informes:

- Informe sobre el estado de cifrado de los dispositivos administrados. Este informe proporciona detalles sobre el cifrado de datos de varios dispositivos administrados. Por ejemplo, el informe muestra el número de dispositivos a los que se aplica la directiva con reglas de cifrado configuradas. Además, puede averiguar, entre otras cosas, cuántos dispositivos deben reiniciarse. El informe también contiene información sobre la tecnología de cifrado y el algoritmo usados en cada dispositivo.
- Informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo. Este informe contiene la misma información que el informe sobre el estado de cifrado de los dispositivos administrados, pero proporciona datos solo para dispositivos de almacenamiento masivo y unidades extraíbles.
- Informe sobre derechos de acceso a unidades cifradas. Este informe muestra qué cuentas de usuario tienen acceso a unidades cifradas.
- Informe sobre los errores de cifrado de archivos. Este informe contiene información sobre errores que ocurrieron durante tareas de cifrado o descifrado de datos en dispositivos.
- Informe sobre el bloqueo de acceso a los archivos cifrados. Este informe contiene información sobre el bloqueo de acceso de las aplicaciones a los archivos cifrados. Este informe es útil si un usuario o una aplicación no autorizados intenta obtener acceso a archivos o unidades cifradas.

Puede generar cualquiera de los informes en la sección **Supervisión e informes** → **Informes**. También puede generar los siguientes informes de cifrado en la sección **Operaciones** → **Protección y cifrado de datos**:

- Informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo
- Informe sobre derechos de acceso a unidades cifradas
- Informe sobre los errores de cifrado de archivos

*Para generar un informe de cifrado en la sección **Protección y cifrado de datos**:*

1. Verifique que la opción **Mostrar protección y cifrado de datos** esté habilitada en las opciones de la interfaz.
2. En el menú principal, vaya a **Operaciones** → **Protección y cifrado de datos**.
3. Abra la sección **Unidades cifradas** para generar el informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo o el informe sobre derechos de acceso a unidades cifradas.
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** → **Unidades cifradas**.

   Aparece una lista de unidades cifradas.
3. Seleccione la unidad a la que el usuario haya solicitado acceso.
4. Haga clic en el botón **Otorgar acceso al dispositivo en modo sin conexión**:
5. En la ventana que se abre, seleccione el complemento correspondiente a la aplicación de Kaspersky que se haya utilizado para cifrar la unidad seleccionada.

   > Si la unidad se cifró 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 sin conexión.
6. Siga las instrucciones proporcionadas en la Ayuda de Kaspersky Endpoint Security para Windows (consulte los bloques de expansión al final de la sección).

Tras hacerlo, el usuario aplica el archivo recibido para acceder a la unidad cifrada y leer los datos almacenados en la unidad.

Usuarios y roles de usuario

En esta sección se explica qué son, cómo se crean y cómo se modifican los usuarios y los roles de usuario. También se brindan instrucciones para asignar roles y grupos a los usuarios y para asociar los roles a perfiles de directivas.

Acerca de 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 solamente se utilizan en Kaspersky Security Center Cloud Console.

Para ver tablas de cuentas de usuario y grupos de seguridad, haga lo siguiente:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos**.
2. Seleccione la pestaña **Usuarios** o **Grupos**.

Se abrirá la tabla de usuarios o grupos de seguridad. De forma predeterminada, la tabla abierta se filtra por las columnas **Subtipo** y **Tiene roles asignados**. La tabla muestra los usuarios o grupos internos que tienen roles asignados.

Si desea ver la tabla solo con las cuentas de los usuarios locales, establezca los criterios de filtro **Subtipo** en **Local**.

Si cambia a un Servidor de administración secundario versión 14.2 o anterior y, a continuación, abre la lista de usuarios o grupos de seguridad, la tabla abierta se filtrará solo por la columna **Subtipo**. El filtro por la columna **Tiene roles asignados** no se aplica de manera predeterminada. La tabla filtrada incluirá todos los usuarios internos o grupos de seguridad con el rol asignado y sin él.

Agregar una cuenta de un usuario interno

Si lo desea, puede agregar usuarios internos de su espacio de trabajo en el portal. Después de agregar un usuario interno, puede asignarle un rol 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 un rol a un conjunto de usuarios o a un conjunto de grupos de seguridad en cualquier nivel en la jerarquía de grupos de administración, Servidores de administración, o al nivel de objetos específicos.

Si administra dispositivos a través de una jerarquía de Servidores de administración que incluye servidores de administración virtuales, tenga en cuenta que puede crear, modificar o eliminar funciones de usuario sólo desde un Servidor de administración físico. Luego, puede propagar las funciones de usuario a los Servidores de administración secundarios, incluidos los virtuales.

Los roles de usuario pueden asociarse a perfiles de directivas. Cuando a un usuario se le asigna un rol, se le conceden los ajustes de seguridad que necesita para cumplir con sus funciones laborales.

Un rol de usuario puede asociarse a los usuarios que trabajan con los dispositivos de un grupo de administración específico.

Alcance de un rol de usuario

El *alcance de un rol de usuario* es una combinación de usuarios y grupos de administración. Los ajustes asociados a un rol de usuario se aplican únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

Ventajas de utilizar roles

Una ventaja de utilizar roles es que evita la necesidad de especificar los ajustes de seguridad de cada dispositivo administrado o de cada usuario por separado. La cantidad de dispositivos y usuarios en una empresa puede ser significativa, pero el número de roles laborales que necesitará de ajustes de seguridad especiales siempre será notablemente menor.

Diferencias con los perfiles de directivas

Los perfiles de directivas son propiedades de una directiva creada para cada aplicación de Kaspersky por separado. Un rol se asocia a muchos perfiles de directivas creados para aplicaciones diferentes. De ese modo, un rol es una manera de unir en un solo lugar los ajustes para un determinado tipo de usuario.

Configurar los derechos de acceso a las funciones de la aplicación. Control de acceso basado en roles

Kaspersky Security Center Cloud Console permite utilizar roles para regular el acceso a sus funciones y a las funciones de las aplicaciones de Kaspersky administradas.

Puede configurar los derechos de acceso a las funciones de la aplicación para los usuarios de Kaspersky Security Center 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

En la siguiente tabla, se enumeran las características y funciones de Kaspersky Security Center Cloud Console junto con los derechos de acceso que se requieren para administrar las tareas, los informes y los ajustes asociados con esas funciones o para realizar las acciones de usuario asociadas con esas funciones.

Para realizar las acciones de usuario que se detallan en la tabla, el usuario debe tener el derecho indicado junto a la acción.

Los derechos **Leer**, **Escribir** y **Ejecutar** son aplicables a cualquier tarea, informe o ajuste de 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**.

El área funcional **Características generales**: **Acceder a objetos sin importar sus ACL** está diseñada con fines de auditoría. Cuando los usuarios obtienen derechos de **Lectura** en esta área funcional, obtienen acceso de **Lectura** completo a todos los objetos y pueden ejecutar cualquier tarea creada en selecciones de dispositivos conectados al Servidor de administración a través del Agente de red con derechos de administrador local (root para Linux). Recomendamos conceder estos derechos con precaución y a un conjunto limitado de usuarios que los necesiten para realizar sus funciones oficiales.

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**	**Escribir**	• Agregar un dispositivo a un grupo de administración: **Escribir** • Eliminar un dispositivo de un grupo de administración: **Escribir** • Agregar un grupo de administración a otro grupo de administración: **Escribir** • Eliminar un grupo de administración de otro grupo de administración: **Escribir**	Ninguno	N/C	N/C
Características generales: **Acceder a objetos sin importar sus ACL**	**Leer**	Obtener acceso de lectura a todos los objetos: **Leer**	Ninguno	N/C	El acceso se otorga sin importar los demás derechos, incluso si se prohíbe el acceso de lectura a

					objetos específicos.
Características generales: **Funcionalidad básica**	• **Leer** • **Escribir** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	• Reglas de movimiento de dispositivos (crear, modificar o eliminar) para el Servidor virtual: **Escribir**, **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** • Agregar, modificar o eliminar la lista de redes definidas por NLA: **Escribir** • 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 sobre 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" • "Informe de vulnerabilidades"	Ninguno

				• "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** • **Escribir**	• Ver objetos eliminados en la Papelera de reciclaje: **Leer** • Eliminar objetos de la Papelera de reciclaje: **Escribir**	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** • **Escribir**	• 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** • **Escribir** • **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"
Características generales: **administración de claves de licencia**	• **Exportar archivo de clave** • **Escribir**	• Exportar un archivo de clave: **Exportar archivo de clave** • Modificar la configuración de la clave de licencia del Servidor de administración: **Escribir**	Ninguno	N/C	N/C
Características generales: **Administración de informes**	• **Leer** • **Escribir**	• 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** • Administrar roles de usuario: **Modificar ACL**	Ninguno	N/C	N/C

		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** • **Escribir** • **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	**Escribir**	Importar las claves de cifrado: **Escribir**	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** • **Leer** • **Escribir** • **Ejecutar**	• 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 estación de trabajo del administrador**	Ninguno	"Informe sobre los usuarios de los dispositivos"	Ninguno

	• **Realizar operaciones en selecciones de dispositivos**				
Administración de sistemas: **Inventario de hardware**	• **Leer** • **Escribir** • **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** • **Escribir**	• 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** • **Escribir** • **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 e imágenes de sistema operativo: **Escribir**	"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** • **Escribir** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	• Ver propiedades de parches de terceros: **Leer** • Cambiar las propiedades de parches de terceros: **Escribir**	• "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** • **Escribir** • **Ejecutar** • **Realizar operaciones en selecciones de dispositivos**	• Ver las propiedades de un paquete de instalación de una aplicación de terceros (con Administración de vulnerabilidades y parches habilitada): **Leer** • Cambiar las propiedades de un paquete de instalación de una aplicación de terceros (con Administración de	Ninguno	N/C	Paquetes de instalación: • "Aplicación personalizada" • "Paquete VAPM"

		vulnerabilidades y parches habilitada): **Escribir**			
Administración de sistemas: **Inventario de software**	• **Leer** • **Escribir** • **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

Los roles de usuario asignados a los usuarios de Kaspersky Security Center Cloud Console les brindan los derechos que necesitan para acceder a las funciones de la aplicación.

A los usuarios creados en un Servidor virtual no se les puede asignar una función en el Servidor de administración.

Puede utilizar roles de usuario predefinidos, que ya vienen configurados con un conjunto de derechos, o puede crear roles nuevos y configurar los derechos necesarios a mano. Algunos de los roles predefinidos de Kaspersky Security Center Cloud Console se pueden asociar a puestos de trabajo específicos; es el caso, por ejemplo, de los roles **Auditor**, **Supervisor** y **Oficial de seguridad**, que están disponibles en Kaspersky Security Center Cloud Console desde la versión 11. Los derechos de acceso de estos roles están preconfigurados para facilitar las obligaciones y las tareas típicas de los puestos asociados. En la siguiente tabla, se muestra cómo estos roles pueden vincularse a puestos de trabajo específicos.

Ejemplos de roles para puestos de trabajo específicos

Rol	Comentario
Auditor	Permite 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	Permite todas las operaciones en las siguientes áreas funcionales: • **Características generales**:

administración	• **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 **Leer** y **Escribir** en el área funcional **Características generales: Administración de claves de cifrado**.
Operador del Servidor de administración	Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales: • **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 controlada** 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 los derechos **Leer** y **Ejecutar** en el área funcional **Características generales: servidores de administración virtuales**.
Operador de instalación	Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales: • **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 **Leer** y **Escribir** en el área funcional **Características generales: Administración de claves de cifrado**.
Operador de Kaspersky Endpoint Security	Otorga los derechos **Leer** y **Ejecutar** en las siguientes áreas funcionales: • **Características generales: funcionalidad básica** • Área de Kaspersky Endpoint Security (se incluyen todas las funciones)
Administrador principal	Permite todas las operaciones en las áreas funcionales, *excepto* las siguientes áreas de **Características generales**: • **Acceder a objetos sin importar sus ACL** • **Administración de informes forzados** Otorga los derechos **Leer** y **Escribir** 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**
	  • **Despliegue 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 Administración de dispositivos móviles	Otorga los derechos **Leer** y **Ejecutar** en el área funcional **Características generales**: **Funcionalidad básica**. 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 controlada** Otorga los derechos **Leer**, **Escribir**, **Ejecutar**, **Guardar archivos de los dispositivos en la estación de trabajo del administrador** y **Realizar operaciones en selecciones de dispositivos** en el área funcional **Administración de sistemas: Conectividad**.

	Puede asignar este rol al responsable de la seguridad de TI de su organización.
Analista de seguridad sénior	Otorga el derechos **Leer** en el área funcional **Características generales**: **funcionalidad básica**. Otorga los derechos **Leer**, **Escribir**, **Ejecutar**, **Guardar archivos de los dispositivos en la estación de trabajo del administrador** y **Realizar operaciones en selecciones de dispositivos** en el área funcional **Administración de sistemas: Conectividad**. 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 **Leer** en las áreas funcionales **Características generales**: **Acceder a objetos sin importar sus ACL** y **Características generales**: **Administración de informes controlada**. 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.
Administrador de Administración de vulnerabilidades y parches	Permite todas las operaciones en las áreas funcionales **Características generales**: **Funcionalidad básica** y **Administración de sistemas** (se incluyen todas las funciones).
Operador de Administración de vulnerabilidades y parches	Otorga los derechos **Leer** y **Ejecutar** (cuando corresponde) en las áreas funcionales **Características generales**: **Funcionalidad básica** y **Administración de sistemas** (se incluyen todas las funciones).

Asignación de derechos de acceso a objetos específicos

Además de asignar derechos de acceso al nivel de servidor, puede configurar el acceso a objetos específicos, por ejemplo, a una tarea específica. La aplicación le permite especificar derechos de acceso a los siguientes tipos de objetos:

- Grupos de administración
- Tareas
- Informes
- Selecciones de dispositivos
- Selecciones de eventos

Para asignar derechos de acceso a un objeto específico:

1. Según el tipo de objeto, en el menú principal vaya a la sección correspondiente:
   - **Activos (dispositivos) → Jerarquía de grupos**
   - **Activos (dispositivos) → Tareas**
   - **Supervisión e informes → Informes**
   - **Activos (dispositivos) → Selecciones de dispositivos**
   - **Supervisión e informes → Selecciones de eventos**
2. Abra las propiedades del objeto al que desea configurar los derechos de acceso.

   Para abrir la ventana de propiedades de un grupo de administración o una tarea, haga clic en el nombre del objeto. Las propiedades de otros objetos se pueden abrir usando el botón en la barra de herramientas.
3. En la ventana de propiedades, abra la sección **Derechos de acceso**.

Se abre la lista de usuarios. Los usuarios y grupos de seguridad enumerados tienen derechos de acceso al objeto. De forma predeterminada, si utiliza una jerarquía de grupos o servidores de administración, la lista y los derechos de acceso se heredan del grupo de administración principal o del servidor principal.

4. Para poder modificar la lista, habilite la opción **Usar permisos personalizados** opción.

5. Configurar derechos de acceso:

   - Use los botones **Agregar** y **Eliminar** para modificar la lista.
   - Especifique los derechos de acceso para un usuario o grupo de seguridad. Realice una de las siguientes acciones:
     - Si desea especificar los derechos de acceso manualmente, seleccione el usuario o grupo de seguridad, haga clic en el botón **Derechos de acceso** y, a continuación, especifique los derechos de acceso.
     - Si desea asignar un rol de usuario al usuario o grupo de seguridad, seleccione el usuario o grupo de seguridad, haga clic en el botón **Roles** y, a continuación, seleccione el rol que desea asignar.

6. Haga clic en el botón **Guardar**.

Los derechos de acceso al objeto se configuran.

Asignar derechos de acceso a usuarios y grupos de seguridad

Puede asignar derechos de acceso a sus usuarios y grupos de seguridad para que puedan utilizar diferentes funciones del Servidor de administración, como Kaspersky Endpoint Security for Linux.

Para asignar derechos de acceso a un usuario o grupo de seguridad, haga lo siguiente:

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

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Derechos de acceso**, marque la casilla ubicada junto al nombre del usuario o del grupo de seguridad al que desea asignar derechos y, luego, haga clic en el botón **Derechos de acceso**.

   No puede seleccionar varios usuarios o grupos de seguridad al mismo tiempo. Si selecciona más de un elemento, el botón **Derechos de acceso** se deshabilitará.

3. Configure el conjunto de derechos para el usuario o grupo:

   a. Amplíe el nodo con funciones del Servidor de administración o de otra aplicación de Kaspersky.

   b. Marque las casillas **Permitir** o **Denegar** ubicadas junto a la función o el derecho de acceso pertinentes.

      Ejemplo 1: Marque la casilla **Permitir** ubicada junto al nodo **Integración de aplicaciones** para otorgar a un usuario o grupo todos los derechos de acceso disponibles para la característica de integración de aplicaciones (**Lectura**, **Escritura** y **Ejecución**).

      Ejemplo 2: Expanda el nodo **Administración de claves de cifrado** y marque la casilla **Permitir** ubicada junto al permiso **Escritura** para otorgar a un usuario o grupo el derecho de acceso **Escritura** para la función de administración de claves de cifrado.

4. Después de configurar el conjunto de derechos de acceso, haga clic en **Aceptar**.

Se configurará el conjunto de derechos para el usuario o grupo de usuarios.

Los permisos del Servidor de administración (o el grupo de administración) se dividen en las siguientes áreas:

- Características generales:
  - Gestión de grupos de administración
  - Acceder a objetos sin importar sus ACL
  - Funcionalidad básica
  - Objetos eliminados
  - Administración de claves de cifrado
  - Procesamiento de eventos
  - Operaciones en el Servidor de administración (solo en la ventana de propiedades del Servidor de administración)
  - Etiquetas de dispositivos
  - Despliegue de la aplicación de Kaspersky
  - Administración de claves de licencia
  - Integración de aplicaciones
  - Administración de informes controlada
  - Jerarquía de Servidores de administración
  - Permisos de usuario
  - Servidores de administración virtuales
- Administración de dispositivos móviles:
  - General
  - Self Service Portal
- Administración de sistemas:
  - Conectividad
  - Ejecutar scripts de forma remota
  - Inventario de hardware
  - Control de acceso a la red
  - Despliegue de sistemas operativos

- Administración de vulnerabilidades y parches
- Instalación remota
- Inventario de software

Si no se selecciona **Permitir** ni **Denegar** para un derecho de acceso, el acceso se considera *indefinido*: el usuario no tendrá ese derecho hasta que se le conceda o deniegue explícitamente.

Los derechos de un usuario son la suma de lo siguiente:

- los propios derechos del usuario
- los derechos de todos los roles asignados al usuario
- los derechos de todo el grupo de seguridad al que pertenece el usuario
- los derechos de todos los roles asignados a los grupos de seguridad a los que pertenece el usuario

Si al menos uno de estos conjuntos de derechos tiene **Denegar** para un permiso, al usuario se le niega este permiso, incluso si otros conjuntos lo permiten o lo dejan sin definir.

También puede agregar usuarios y grupos de seguridad al alcance de un rol de usuario para usar diferentes funciones del Servidor de administración. La configuración asociada a un rol de usuario se aplica únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

Asignación de un rol a un usuario o a un grupo de seguridad

Para asignar un rol a un usuario o grupo de seguridad, haga lo siguiente:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos**, y luego seleccione la pestaña **Usuarios** o **Grupos**.
2. Seleccione el nombre del usuario o del grupo de seguridad a quien desea asignar un rol.

   Puede seleccionar varios nombres.
3. En la línea del menú, haga clic en el botón **Asignar rol**.

   Se inicia el asistente de asignación de roles.
4. Siga las instrucciones del asistente: seleccione el rol que desea asignar a los usuarios o grupos de seguridad seleccionados, y elija el alcance del rol.

   El *alcance de un rol de usuario* es una combinación de usuarios y grupos de administración. Los ajustes asociados a un rol de usuario se aplican únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

El rol con un conjunto de derechos para trabajar con el Servidor de administración se asigna al usuario (o usuarios, o al grupo de seguridad). En la lista de usuarios o grupos de seguridad, aparece una casilla en la columna **Tiene roles asignados**.

Creación de roles de usuario

Para crear un rol de usuario:

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.
2. Haga clic en **Agregar**.
3. En la ventana **Nombre del nuevo rol** que se abre, introduzca el nombre del nuevo rol.
4. Haga clic en **Aceptar** para aplicar los cambios.
5. Cuando se abra la ventana de propiedades del rol, cambie la configuración del rol:
   - En la pestaña **General**, modifique el nombre del rol.
     No es posible modificar el nombre de los roles predefinidos.
   - En la pestaña **Configuración**, modifique el alcance del rol, así como las directivas y los perfiles asociados al rol.
   - En la pestaña **Derechos de acceso**, modifique los derechos de acceso a las aplicaciones de Kaspersky.
6. Haga clic en **Guardar** para guardar los cambios.

El nuevo rol aparece en la lista de roles de usuario.

Editar un rol de usuario

Para editar un rol de usuario:

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.
2. Haga clic en el nombre del rol que desee editar.
3. Cuando se abra la ventana de propiedades del rol, cambie la configuración del rol:
   - En la pestaña **General**, modifique el nombre del rol.
     No es posible modificar el nombre de los roles predefinidos.
   - En la pestaña **Configuración**, modifique el alcance del rol, así como las directivas y los perfiles asociados al rol.
   - En la pestaña **Derechos de acceso**, modifique los derechos de acceso a las aplicaciones de Kaspersky.
4. Haga clic en **Guardar** para guardar los cambios.

El rol actualizado aparece en la lista de roles de usuario.

Editar el alcance de un rol de usuario

El *alcance de un rol de usuario* es una combinación de usuarios y grupos de administración. Los ajustes asociados a un rol de usuario se aplican únicamente a los dispositivos que pertenecen a los usuarios que tienen ese rol, y solo cuando esos dispositivos pertenecen a grupos y subgrupos asociados al rol en cuestión.

Para agregar usuarios, grupos de 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 roles** → **Usuarios y grupos**, y luego seleccione la pestaña **Usuarios** o **Grupos**.
2. Seleccione las casillas de verificación ubicadas junto a los usuarios o grupos de usuarios que desee agregar al alcance del rol de usuario.
3. Haga clic en el botón **Asignar rol**.

   Se inicia el asistente de asignación de roles. Avance por el asistente utilizando el botón **Siguiente**.
4. En el paso **Seleccionar rol**, seleccione el rol de usuario que desee asignar.
5. En el paso **Definir alcance**, seleccione el grupo de administración que desee agregar al alcance del rol de usuario.
6. Haga clic en el botón **Asignar rol** para cerrar la ventana.

Los usuarios o grupos de usuarios y el grupo de administración seleccionados se agregan al alcance del rol de usuario.

Método 2:

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.
2. Haga clic en el nombre del rol cuyo alcance desee definir.
3. Cuando se abra la ventana de propiedades del rol, seleccione la pestaña **Configuración**.
4. En la sección **Alcance del rol**, haga clic en **Agregar**.

   Se inicia el asistente de asignación de roles. Avance por el asistente utilizando el botón **Siguiente**.
5. En el paso **Definir alcance**, seleccione el grupo de administración que desee agregar al alcance del rol de usuario.
6. En el paso **Seleccionar usuarios**, seleccione los usuarios y los grupos de seguridad que desee agregar al alcance del rol de usuario.
7. Haga clic en el botón **Asignar rol** para cerrar la ventana.
8. Cierre la ventana de propiedades del rol.

Los usuarios o grupos de usuarios y el grupo de administración seleccionados se agregan al alcance del rol de usuario.

Método 3:

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

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Derechos de acceso**, marque la casilla junto al nombre del usuario o del grupo de seguridad que desea agregar al alcance de un rol de usuario y, luego, haga clic en el botón **Roles**.

   No puede seleccionar varios usuarios o grupos de seguridad al mismo tiempo. Si selecciona más de un elemento, el botón **Roles** se deshabilitará.

3. En la ventana **Roles**, seleccione el rol de usuario que desea asignar, haga clic en **Aceptar** y guarde los cambios.

   Los usuarios o grupos de seguridad seleccionados se agregan al alcance del rol de usuario.

Eliminar un rol de usuario

Para eliminar un rol de usuario:

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.
2. Marque la casilla ubicada junto al nombre del rol que desee eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic en **Aceptar**.

Se elimina el rol de usuario.

Asociación de perfiles de directivas con roles

Los roles de usuario pueden asociarse a perfiles de directivas. Al crear una asociación entre un perfil de directiva y un rol, la regla de activación del perfil pasa a depender del rol y, en consecuencia, el perfil de directiva se activa para los usuarios que tienen el rol especificado.

A modo de ejemplo, suponga que los dispositivos de un grupo de administración, llamado Usuarios, están sujetos a una directiva que prohíbe el uso de aplicaciones de navegación GPS. Existe un solo dispositivo en el grupo que necesita contar con un navegador GPS: el dispositivo que le pertenece al mensajero. En esta situación, puede asignar un rol llamado "Mensajero" al propietario de este dispositivo y crear un perfil de directiva que permita utilizar aplicaciones de navegación GPS solo en aquellos dispositivos que pertenezcan a usuarios con el rol "Mensajero". Los demás ajustes de la directiva se mantendrán sin cambios. Solo el usuario que tenga el rol "Mensajero" podrá ejecutar el software de navegación GPS. Si posteriormente se le asigna el rol "Mensajero" a otro empleado más, esa persona también podrá ejecutar aplicaciones de navegación en el dispositivo que le provea la organización. El software de navegación GPS seguirá estando prohibido en los demás dispositivos del grupo de administración.

Para asociar un rol con un perfil de directiva:

1. En el menú principal, vaya a **Usuarios y roles** → **Roles**.
2. Haga clic en el nombre del rol que desee asociar con un perfil de directiva.

Se abre la ventana de propiedades del rol, con la pestaña **General** seleccionada.

3. Seleccione la pestaña **Configuración** y desplácese hacia abajo hasta llegar a la sección **Directivas y perfiles**.
4. Haga clic en **Editar**.
5. Asocie el rol con un perfil de directiva nuevo o existente:
   - Para asociar el rol con **un perfil de directiva existente**, haga clic en el corchete angular (>) ubicado junto al nombre de la directiva pertinente, busque el nombre del perfil con el que quiera asociar el rol y active la casilla adyacente a ese perfil.
   - Para asociar el rol con **un nuevo perfil de directiva**:
     a. Marque la casilla adyacente a la directiva para la que se vaya a crear el perfil.
     b. Haga clic en **Nuevo perfil de directiva**.
     c. Escriba el nombre del nuevo perfil y configure sus opciones.
     d. Haga clic en el botón **Guardar**.
     e. Marque la casilla adyacente al nuevo perfil.
6. Haga clic en **Asignar a rol**.

El perfil quedará asociado al rol y aparecerá en las propiedades del rol. El perfil se aplicará automáticamente al dispositivo de toda persona que tenga asignado el rol.

Crear un grupo de seguridad

Para crear un grupo de seguridad:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Grupos**.
2. Haga clic en **Nuevo grupo**.
3. En la ventana **Nuevo grupo**, especifique la siguiente configuración para el nuevo grupo de seguridad:
   - **Nombre**
   - **Descripción**
4. Haga clic en **Aceptar** para guardar los cambios.

Se agrega un nuevo grupo de seguridad a la lista de grupos de seguridad.

Editar un grupo de seguridad

Para editar un grupo de seguridad:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Grupos**.
2. Haga clic en el nombre del grupo de seguridad que desee editar.
3. Cuando se abra la ventana de configuración del grupo, cambie la configuración del grupo de seguridad:
   - En la pestaña **General**, puede cambiar la configuración de **Nombre** y **Descripción**. Estas configuraciones están disponibles solo para grupos de seguridad internos.
   - En la pestaña **Usuarios**, puede agregar usuarios al grupo de seguridad. Esta configuración solo está disponible para usuarios internos y grupos de seguridad internos.
   - En la pestaña **Roles**, puede asignar un rol al grupo de seguridad.
4. Haga clic en **Guardar** para guardar los cambios.

Los cambios se aplican al grupo de seguridad.

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 roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Active las casillas de verificación ubicadas junto a las cuentas de usuario que desee agregar al grupo.
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 agregar usuarios internos a un grupo mediante la configuración del grupo.

Eliminar un grupo de seguridad

Solo es posible eliminar grupos de seguridad internos.

Para eliminar un grupo de usuarios, haga lo siguiente:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Grupos**.
2. Marque la casilla de verificación ubicada junto al grupo de usuarios que desee eliminar.

3. Haga clic en **Eliminar** y luego confirme la eliminación en la ventana abierta.

Se elimina el grupo de usuarios.

Configurar la integración de ADFS

Para que los usuarios que se encuentren registrados en Active Directory (AD) en su organización puedan iniciar sesión en Kaspersky Security Center Cloud Console, debe configurar la integración de 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 contar con el derecho de acceso que permite cambiar permisos de usuario.

Antes de continuar, asegúrese de completar un sondeo de Active Directory.

Para configurar la integración de AD FS:

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

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, seleccione la sección **Configuración de 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, agregue un nuevo grupo de aplicaciones y, a continuación, seleccione la plantilla **Server application** para agregar una nueva aplicación (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 Propiedades del Servidor de administración.

6. Genere un secreto de cliente. Necesitará el secreto de cliente para configurar la integración en Kaspersky Security Center Cloud Console.

7. Guarde las propiedades de la aplicación agregada.

8. Agregue una nueva aplicación al grupo de aplicaciones creado. Esta vez, seleccione la plantilla **Web API**.

9. En la pestaña **Identifiers**, busque la lista **Relying party identifiers** y agregue el id. de cliente de la aplicación de servidor que agregó antes.

10. En la pestaña **Client Permissions**, busque la lista **Permitted scopes** y seleccione los alcances **allatclaims** y **openid**.

11. En la pestaña **Issuance Transform Rules**, elija la plantilla **Send LDAP Attributes as Claims** y agregue una nueva plantilla:

    a. Asigne un nombre a la regla. Por ejemplo, puede asignarle el nombre "SID del grupo".

    b. Seleccione **Active Directory** como almacén de atributos y, a continuación, cree un vínculo entre **Token-Groups as SIDs** como atributo LDAP y "SID de grupo" como tipo de notificación saliente.

12. En la pestaña **Issuance Transform Rules**, seleccione la plantilla **Send Claims Using a Custom Rule** y agregue una nueva regla:

    a. Asigne un nombre a la regla. Por ejemplo, puede asignarle el nombre "ActiveDirectoryUserSID".

    b. En el campo **Custom rule**, escriba lo siguiente:

```
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 Habilitada**.

15. Haga clic en el vínculo **Configuración** y, a continuación, elija el archivo que contiene el certificado (o los certificados) del servidor de federación.

16. Haga clic en el vínculo **Configuración de integración con ADFS** y configure los siguientes ajustes:

- **URL del emisor**

  La dirección URL del servidor de federación que utiliza en su organización.

  En particular, Kaspersky Security Center Cloud Console agrega "/.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 a Kaspersky Security Center Cloud Console. Encontrará el id. de cliente en la consola de administración de AD FS, dentro de la ventana de propiedades de la aplicación de servidor correspondiente a Kaspersky Security Center Cloud Console.

- **Secreto del cliente**

  Generó un secreto de cliente en la consola de administración de AD FS al especificar las propiedades de la aplicación de servidor correspondiente a Kaspersky Security Center Cloud Console.

- **Dominio desde el cual autenticar a los usuarios**

Los miembros del dominio que seleccione podrán iniciar sesión en Kaspersky Security Center Cloud Console con sus credenciales de cuenta de dominio. Los nombres de dominio aparecerán en la lista una vez que se complete el sondeo de la red.

- **Nombre del 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 se necesita para identificar al usuario en Kaspersky Security Center Cloud Console. De forma predeterminada, el nombre del campo en el token de id. es "primarysid".

- **Nombre del 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 se llama "groupid" en el token de id.

17. Haga clic en el botón **Guardar**.

    Se completó la integración de AD FS. Para iniciar sesión en Kaspersky Security Center Cloud Console con las credenciales de una cuenta de AD, utilice el vínculo que encontrará en la sección **Configuración de integración con ADFS** (**Vínculo de inicio de sesión en Kaspersky Security Center Cloud Console con ADFS**).

La primera vez que inicie sesión en Kaspersky Security Center Cloud Console a través de AD FS, la consola podría tardar más de lo usual en responder.

Configurar la integración con Microsoft Entra ID

Debe configurar la integración con Microsoft Entra ID para permitir que los usuarios de su organización inicien sesión en Kaspersky Security Center Cloud Console con las credenciales de su 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:

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

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, vaya a la sección **Microsoft Entra ID**.

3. Active el interruptor **Integración con Microsoft Entra ID**.

4. Copie los vínculos de los siguientes campos:

   - **URL de devolución de llamada**

- **URL de cierre de sesión del canal frontal**

  Necesitará estas URL para registrar Kaspersky Security Center Cloud Console en el inquilino de Microsoft Entra ID.

- **URL de inicio de sesión**

  Necesitará esta URL para permitir que los usuarios inicien 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, seleccione el inquilino de su organización.

   Debe tener el rol de administrador global o administrador de aplicaciones en el inquilino.

6. En el menú principal, vaya a **Identidad** → **Aplicaciones** → **Registros de aplicaciones** y haga clic en el botón **Nuevo registro**.

7. En la ventana que se abre, haga lo siguiente:

   - Especifique un nombre para la aplicación Kaspersky Security Center Cloud Console.
   - En la sección **Tipos de cuenta compatibles**, seleccione la opción **Cuentas solo de este directorio organizativo (solo <nombre_inquilino>: inquilino único)**.
   - En la sección **URI de redireccionamiento**, seleccione **Web** en la lista desplegable y, luego, ingrese 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, agregue 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 usar la URL de inicio de sesión.

10. Copie el **ID de la aplicación (cliente)** y el **ID del directorio (inquilino)** y guárdelos de la manera que le resulte más conveniente.

    Necesitará estos ID para 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** e ingrese las URL que copió de Kaspersky Security Center Cloud Console en el paso 4:

    - En la sección **Web**, haga clic en el botón **Agregar URI** y, luego, ingrese la URL de inicio de sesión.
    - En la sección **URL de cierre de sesión del canal frontal**, ingrese 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 haga lo siguiente:

    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 una descripción para el secreto del cliente y seleccione el período tras el cual caduca el secreto.

Le recomendamos que copie la fecha de caducidad del secreto, como considere conveniente, para rotar los secretos de forma 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**.

Recomendamos que copie la información inmediatamente después de crear el secreto del cliente.

13. el menú de la aplicación Kaspersky Security Center Cloud Console, vaya a la sección **Configuración del token** y haga lo siguiente:

- Agregue la declaración opcional **onprem_sid**:

  a. Haga clic en el botón **Agregar declaración opcional**.

  b. En la ventana que se abre, seleccione el tipo de token **ID** y, en la columna **Declaración**, seleccione la casilla junto a **onprem_sid**.

  c. Haga clic en el botón **Agregar**.

  La declaración opcional **onprem_sid** se muestra en la página **Declaraciones opcionales**.

- Agregue la declaración opcional **preferred_username**:

  a. Haga clic en el botón **Agregar declaración opcional**.

  b. En la ventana que se abre, seleccione el tipo de token **Acceso** y, en la columna **Declaración**, seleccione la casilla junto a **preferred_username**.

  c. Haga clic en el botón **Agregar**.

  La declaración opcional **preferred_username** se muestra en la página **Declaraciones opcionales**.

14. En el menú de la aplicación Kaspersky Security Center Cloud Console, vaya a la sección **Permisos de la API** y agregue los siguientes permisos:

- **User.Read.All**
- **User.Export.All**
- **GroupMember.Read.All**
- **Directory.Read.All**

Para agregar un permiso, haga lo siguiente:

a. Haga clic en el botón **Agregar un permiso** y seleccione la pestaña **API de Microsoft**.

b. Seleccione **Microsoft Graph** → **Permisos de la aplicación** y seleccione el permiso que desea agregar.

c. Haga clic en el botón **Agregar permiso**.

Los cuatro permisos se agregan y se muestran en la página **Permisos configurados**.

d. Haga clic en **Otorgar consentimiento de administrador para <nombre_inquilino>** y, en la ventana que se abre, haga clic en **Sí** para confirmar la concesión del consentimiento para los permisos que agregó.

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 se muestre 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 roles** → **Usuarios y grupos** para asegurarse de que los usuarios y grupos de Microsoft Entra ID se agreguen a Kaspersky Security Center Cloud Console.

   Si los usuarios y grupos de su inquilino de Microsoft Entra ID están sincronizados desde Active Directory de su organización y el sondeo de Active Directory está configurado, los usuarios y grupos ya se agregaron a Kaspersky Security Center Cloud Console como resultado del sondeo de Active Directory.

   De lo contrario, debe habilitar y ejecutar el sondeo de Microsoft Entra ID para agregar los usuarios y grupos de su inquilino de Microsoft Entra ID a Kaspersky Security Center Cloud Console.

2. Asigne los roles necesarios a los usuarios y grupos.

   Para asignar funciones a un usuario en un Servidor de administración virtual, en el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos**, y luego seleccione la pestaña **Usuarios**. Si selecciona la pestaña **Grupos** y, luego, asigna roles 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. Ingresarán esta URL para **iniciar sesión en el espacio de trabajo de Kaspersky Security Center Cloud Console con 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.

Habilitar el sondeo de Microsoft Entra ID

Debe habilitar el sondeo de Microsoft Entra ID para agregar los usuarios de Microsoft Entra ID a Kaspersky Security Center Cloud Console.

Para habilitar el sondeo de Microsoft Entra ID:

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

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, vaya a la sección **Microsoft Entra ID**.

3. En la sección **Detección de usuarios**, active el interruptor **Sondeo de Microsoft Entra ID**.

4. Si desea cambiar la programación de sondeo predeterminada, haga clic en el botón **Configuración de la programación**, especifique la frecuencia y la hora de 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 de inmediato, haga clic en el botón **Ejecutar ahora**.

   Los usuarios se están cargando. Una vez que se cargan los usuarios, el sondeo de Microsoft Entra ID finaliza.

6. Haga clic en el botón **Guardar**.

El sondeo de Microsoft Entra ID se completa y los usuarios de Microsoft Entra ID se agregan a Kaspersky Security Center Cloud Console.

Agregar Kaspersky Security Center Cloud Console a la lista de aplicaciones

Para que los usuarios abran Kaspersky Security Center Cloud Console, puede permitir que hagan clic en el nombre de la aplicación en la lista sin ingresar la URL de inicio de sesión. La lista de aplicaciones está disponible en Mis aplicaciones y el iniciador de Office 365.

Para agregar 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**, ingrese la URL de inicio de sesión.

   b. Si es necesario, en el campo **Cargar nuevo logotipo**, agregue una imagen que se usará como el ícono 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**:

   - **¿Habilitado 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 **Agregar usuario/grupo** y, luego, haga clic en el vínculo que se encuentra 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 el nombre de la aplicación en la lista sin ingresar la URL de inicio de sesión.

Designación de un usuario como propietario de un dispositivo

Si busca información para designar a un usuario como propietario de un dispositivo móvil, consulte la Ayuda de Kaspersky Security for Mobile.

Para designar a un usuario como propietario de un dispositivo:

1. Si desea asignar un propietario de un dispositivo conectado a un Servidor de administración virtual, primero cambie al Servidor de administración virtual:

   a. En el menú principal, haga clic en el ícono de corchete ( ) a la derecha del nombre del Servidor de administración actual.

   b. Seleccione el Servidor de administración requerido.

2. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.

   Se abre una lista de usuarios. Si actualmente está conectado a un Servidor de administración virtual, la lista incluye usuarios del Servidor de administración virtual actual y el Servidor de administración principal.

3. Haga clic en el nombre de la cuenta de usuario que desee designar como propietario del dispositivo.

4. En la ventana que se abre con la configuración del usuario, seleccione la pestaña **Dispositivos**.

5. Haga clic en **Agregar**.

6. En la lista de dispositivos, seleccione el dispositivo que desee asignar al usuario.

7. Haga clic en **Aceptar**.

   El dispositivo seleccionado se agrega a la lista de dispositivos asignados al usuario.

Como alternativa para realizar esta operación, ingrese a **Activos (dispositivos)** → **Dispositivos administrados**, haga clic en el nombre del dispositivo que desee asignar y luego haga clic en el vínculo **Administrar propietario del dispositivo**.

Asignar a un usuario como propietario del dispositivo tras instalar el Agente de red

Para permitir que el usuario se registre como propietario de un dispositivo Linux:

1. En Kaspersky Security Center Web Console, vaya a **Descubrimiento y despliegue** → **Despliegue y asignación** → **Paquetes de instalación**.

   Se abrirá la lista de paquetes de instalación.

2. Haga clic en el paquete de instalación del Agente de red.

   Se abrirá la ventana de propiedades del paquete de instalación.

3. En la ventana de propiedades del paquete de instalación, haga clic en **Configuración** → **Avanzado**.

4. En la sección **Registro de usuario como propietario de un dispositivo (solo Linux)**, active la opción **Permitir la ejecución de la utilidad de registro de usuario luego de la instalación del Agente de red** y haga clic en **Guardar**.

La utilidad para registrar al usuario como propietario del dispositivo se puede ejecutar a través de la línea de comandos en el dispositivo cliente.

Para registrar un usuario como propietario de un dispositivo Linux en el dispositivo cliente:

1. Ejecute el siguiente comando en la línea de comandos del dispositivo cliente:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. Ingrese el nombre de usuario y la contraseña, si se le solicitan estos datos.

   Si el nombre de usuario y la contraseña están incluidos en el archivo de respuesta o en el paquete de instalación del Agente de red, ejecute el siguiente comando en la línea de comandos del dispositivo cliente:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

Si el usuario forma parte de un grupo de seguridad interno, el nombre de usuario debe ser el mismo.

Si el usuario forma parte de un grupo de seguridad de Active Directory, el nombre de usuario debe constar del nombre de usuario y el nombre de dominio.

Se registrará al usuario 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.

Puede administrar revisiones de los siguientes objetos:

- Propiedades del Servidor de administración
- Directivas
- Tareas
- Grupos de administración
- Cuentas de usuario
- Paquetes de instalación

Puede realizar las siguientes acciones con las revisiones de los objetos:

- Ver una revisión seleccionada (disponible solo para directivas)
- Revertir los cambios realizados en un objeto a una revisión seleccionada
- Guardar revisiones como archivo JSON (disponible solo para directivas)

Todo objeto compatible con la administración de revisiones tiene una sección llamada **Historial de revisiones** en su ventana de propiedades. La sección contiene una lista de revisiones asociadas al objeto y los siguientes datos:

- **Revisión** número de revisión del objeto.
- **Hora** fecha y hora de modificación del objeto.
- **Usuario** nombre del usuario que modificó el objeto.
- **Dirección IP del dispositivo del usuario**: dirección IP del dispositivo desde el que se modificó el objeto.
- **Dirección IP de Web Console**: dirección IP de Kaspersky Security Center Web Console con la que se modificó el objeto.
- **Acción** acción realizada en el objeto.
- **Descripción** descripción de la revisión vinculada al cambio en la configuración del objeto.

  De forma predeterminada, la descripción de las revisiones está en blanco. Para agregar una descripción a una revisión, seleccione la revisión pertinente y haga clic en el botón **Editar descripción**. En la ventana abierta, ingrese un texto que describa la revisión.

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 revisiones**.
2. En la lista de revisiones del objeto, seleccione el número de revisión a la 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 revisiones**.
2. En la lista de revisiones del objeto, seleccione la revisión a la que desea agregar la descripción.
3. Haga clic en el botón **Editar descripción**.
   Se abre la ventana **Descripción**.
4. En la ventana **Descripción**, ingrese un texto que describa la revisión.
   De forma predeterminada, la descripción de las revisiones está en blanco.
5. Guarde la descripción de la revisión.

Se agrega la descripción a la revisión del objeto.

Ver y guardar una revisión de una directiva

Kaspersky Security Center 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.

Para que pueda ver y guardar la revisión de una directiva, el complemento web de administración correspondiente debe ofrecerle esta prestación.

Para ver una revisión de una directiva:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles**.

2. Haga clic en la directiva a la que corresponda la revisión que desee ver y vaya a la sección **Historial de revisiones**.

3. En la lista de revisiones de la directiva, haga clic en el número de revisión que desee ver.

   Si el tamaño de 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 mostrará un informe en formato HTML con la configuración de la revisión de directiva seleccionada. Dado que el informe se muestra en una ventana emergente, asegúrese de que las ventanas emergentes estén permitidas en su navegador.

Para guardar la revisión de una directiva en un archivo JSON:

En la lista de revisiones de la directiva, seleccione la revisión que desee guardar y luego haga clic en **Guardar en archivo**.

La revisión se guardará en un archivo JSON.

Kaspersky Security Network (KSN)

En esta sección se describe cómo usar la infraestructura de servicios en línea llamada Kaspersky Security Network (KSN). Aquí encontrará información detallada sobre KSN e instrucciones para habilitar KSN, configurar el acceso a KSN y ver las estadísticas de uso del servidor proxy de KSN.

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

Acerca de KSN

Kaspersky Security Network (KSN) es una infraestructura de servicios en línea que brinda acceso a la base de conocimientos en línea de Kaspersky, que contiene información sobre la reputación de los archivos, los recursos web y el software. El uso de los datos de Kaspersky Security Network garantiza una respuesta más rápida de las aplicaciones de Kaspersky ante las amenazas, mejora la eficacia de algunos componentes de protección y reduce el riesgo de falsos positivos. KSN hace posible utilizar las bases de datos de reputación de Kaspersky para obtener información sobre las aplicaciones instaladas en los dispositivos cliente.

Al participar en KSN, acepta enviar a Kaspersky, de manera automática, información sobre el funcionamiento de las aplicaciones de Kaspersky instaladas en los dispositivos cliente administrados mediante Kaspersky Security Center Cloud Console. La información se transfiere de conformidad con la configuración de acceso a KSN. Los analistas de Kaspersky realizan un examen adicional de la información recibida y la suman a las bases de datos de estadísticas y de reputación de Kaspersky Security Network.

La aplicación le preguntará si desea unirse a KSN cuando ejecute el asistente de inicio rápido. Puede iniciar o detener el uso de KSN en cualquier momento cuando use la aplicación.

Utiliza KSN de acuerdo con la Declaración de KSN que lee y acepta cuando habilita KSN. Si se actualiza la Declaración de KSN, se le 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 habilitado, Kaspersky Security Center Cloud Console comprueba que haya acceso a los servidores de KSN. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos. Esto se hace para garantizar que los dispositivos administrados no vean afectado su nivel de seguridad.

Los dispositivos cliente administrados por el Servidor de administración interactúan con KSN mediante el servidor proxy de KSN. El servidor proxy de KSN proporciona las funciones siguientes:

- Permite que los dispositivos cliente envíen solicitudes 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 Habilitado**.

   KSN queda habilitado.

   Si se habilita el botón de activación, los dispositivos cliente enviarán los resultados de instalación de parches a Kaspersky. Al seleccionar este botón de activación, debe leer y aceptar los términos de la Declaración de KSN.

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 Deshabilitado**.

   KSN queda deshabilitado.

   Si se deshabilita este botón de activación, los dispositivos cliente no enviarán los resultados de instalación del parche 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 el menú principal, haga clic en el ícono de configuración ( ) ubicado junto al nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, seleccione la sección **Configuración de 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 mostrará de manera automática cuando abra 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 tarde.

Para ver y luego aceptar o rechazar una Declaración de KSN actualizada:

1. Haga clic en el vínculo **Ver notificaciones** en la esquina superior derecha de la ventana principal de la aplicación.

   Se abre la ventana **Notificaciones**.

2. Haga clic en el enlace **Ver la Declaración de KSN actualizada**.

   Se abre la ventana **Actualización de la Declaración de Kaspersky Security Network**.

3. Lea la Declaración de KSN y haga clic en el botón que responda a su decisión:

   - **Acepto la Declaración de KSN actualizada**
   - **Utilizar KSN con la antigua Declaración**

Según su elección, KSN sigue funcionando de acuerdo con los términos de la Declaración de KSN actual o actualizada. Puede ver el texto de la Declaración de KSN aceptada en las propiedades del Servidor de administración en cualquier momento.

Verificar si el punto de distribución opera como servidor proxy de KSN

Puede habilitar un servidor proxy de KSN en un dispositivo administrado asignado para funcionar como punto de distribución. Para funcionar como proxy de KSN, el dispositivo administrado debe tener activo el servicio ksnproxy. Puede verificar, activar o desactivar este servicio en el dispositivo localmente.

El dispositivo designado como punto de distribución puede utilizar Windows o Linux. El modo de llevar a cabo la verificación en el punto de distribución depende del sistema operativo instalado en el punto de distribución.

Para comprobar si el punto de distribución basado en Windows está operando como servidor proxy de KSN:

1. En el dispositivo de punto de distribución, en Windows, abra **Servicios** (**Todos los programas** → **Herramientas administrativas** → **Servicios**).

2. En la lista de servicios, verifique si el servicio ksnproxy se está ejecutando.

   Si el servicio ksnproxy se está ejecutando, entonces el Agente de red del dispositivo participa en Kaspersky Security Network y funciona como servidor proxy de KSN para los dispositivos administrados incluidos en el alcance del punto de distribución.

Si lo desea, puede desactivar el servicio ksnproxy. En este caso, el Agente de red del punto de distribución deja de participar en Kaspersky Security Network. Esto requiere derechos de administrador local.

Para verificar si un punto de distribución con Linux opera como servidor proxy de KSN:

1. En el dispositivo que actúe como punto de distribución, abra la lista de procesos en ejecución.

2. 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**.

Acercad de la eliminación de dispositivos cliente

Cuando elimina un dispositivo administrado de un grupo de administración, la aplicación mueve el dispositivo al grupo de Dispositivos no asignados. Después de eliminar el dispositivo, las aplicaciones de Kaspersky instaladas (Agente de red y cualquier aplicación de seguridad, por ejemplo, Kaspersky Endpoint Security) permanecen en el dispositivo.

Kaspersky Security Center Cloud Console gestiona los dispositivos en el grupo de Dispositivos no asignados de acuerdo con 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 marca la casilla **Comprendo el riesgo y deseo eliminar el dispositivo** en la ventana de confirmación que se abre cuando elimina dichos dispositivos (ya sea del grupo **Dispositivos no asignados** o **Dispositivos administrados**), significa que está al tanto de la subsecuente eliminación de datos.

  Para descifrar la unidad, se deben cumplir las siguientes condiciones:

  - El dispositivo se vuelve a conectar al Servidor de administración para restaurar los datos necesarios para descifrar la unidad.
  - El usuario del dispositivo recuerda la contraseña de descifrado.
  - La aplicación de seguridad que se usó para cifrar la unidad, por ejemplo, Kaspersky Endpoint Security para Windows, todavía está instalada en el dispositivo.

  Si la tecnología Kaspersky Disk Encryption descifró la unidad, también puede intentar recuperar los datos con la utilidad de restauración FDERT.

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 servidor de administración aún puede ver el dispositivo y configuró un sondeo de red regular, Kaspersky Security Center Cloud Console descubre el dispositivo durante el sondeo de red y lo vuelve a agregar al grupo de 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
- Las aplicaciones de Kaspersky instaladas, incluidas las aplicaciones de seguridad y los componentes de Kaspersky Security Center Cloud Console

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

Escenario: Actualización regular de las bases de datos y las 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. Si ya terminó de configurar la protección de su red, puede enfocarse en mantener el sistema de protección en condiciones. El mantenimiento es fundamental para que los dispositivos administrados se mantengan a salvo de virus, ataques de red, ataques de phishing y otras amenazas.

Existen distintos esquemas para instalar las actualizaciones para los componentes de Kaspersky Security Center Cloud Console y las aplicaciones de seguridad. Elija el o los esquemas que se ajusten a los requisitos de su red.

En el esquema que aquí se describe, las actualizaciones se descargan en los repositorios de los puntos de distribución. Si sus dispositivos administrados no tienen conexión con los puntos de distribución, puede actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky de forma manual o puede hacer que las actualizaciones se tomen directamente de los servidores de Kaspersky.

Al concluir este escenario, los resultados serán los siguientes:

- Los componentes de Kaspersky Security Center Cloud Console se actualizarán automáticamente o solo cuando usted asigne el estado *Aprobada* a las actualizaciones.
- Las bases de datos, los módulos de software y las aplicaciones de seguridad de Kaspersky se actualizarán siguiendo una programación definida por usted. De forma predeterminada, las aplicaciones de seguridad de Kaspersky instalarán únicamente las actualizaciones que usted apruebe.

Puede configurar el proceso de actualización para que las actualizaciones se descarguen e instalen de dos maneras:

- Automática

  Si elige esta opción, solamente tendrá que completar los pasos de este escenario una vez. Tendrá que definir una programación para la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* (de existir esta tarea) y para las tareas de actualización de las aplicaciones de seguridad de Kaspersky. No se requieren cambios en los ajustes de actualización que se encuentran en las propiedades del Agente de red.

- Manual

Puede configurar el proceso de actualización para que se deban ejecutar manualmente la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* (de existir) y las tareas de actualización de las aplicaciones de seguridad de Kaspersky. También puede modificar la configuración del Agente de red para que las actualizaciones de los componentes de Kaspersky Security Center Cloud Console se instalen únicamente si el estado de estas actualizaciones es *Aprobada*.

Requisitos previos

Antes de comenzar, compruebe que hizo lo siguiente:

1. Desplegó las aplicaciones de seguridad de Kaspersky en los dispositivos administrados siguiendo las instrucciones del escenario para desplegar aplicaciones de Kaspersky a través de Kaspersky Security Center 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. Creó y configuró todas las directivas, perfiles de directivas y tareas que se requieren según el escenario para configurar la protección de red.

Etapas

El proceso para configurar la actualización periódica de las bases de datos y las aplicaciones de Kaspersky se divide en etapas:

1. **Crear una tarea para descargar las actualizaciones en los repositorios de los puntos de distribución**

   Crear la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*. Cuando se ejecuta esta tarea, Kaspersky Security Center Cloud Console hace que los puntos de distribución descarguen las actualizaciones directamente de los servidores de actualizaciones de Kaspersky.

   Instrucciones: Crear 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 habilitada en las propiedades de todos los puntos de distribución pertinentes. Si no habilita esta opción para algún punto de distribución, los dispositivos incluidos en su alcance solo podrán obtener actualizaciones de un recurso local o de los servidores de actualizaciones de Kaspersky.

   Si desea que los dispositivos administrados reciban sus actualizaciones solamente de los puntos de distribución, habilite la opción **Distribuir archivos solo a través de los puntos de distribución** en la directiva del Agente de red.

3. **Habilitar el uso de archivos diff para optimizar el proceso de actualización (opcional)**

   Si habilita esta función, se reducirá el volumen de tráfico entre los puntos de distribución y los dispositivos administrados. Para usar esta función, habilite la opción **Descargar archivos diff** en las propiedades de la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*.

   Instrucciones: Utilización de archivos diff para actualizar las bases de datos y los módulos de software de Kaspersky

4. **Seleccionar las actualizaciones que se instalarán**

   De forma predeterminada, las actualizaciones de software descargadas tienen el estado *Sin definir*. Para indicar si una actualización debe o no instalarse en los dispositivos de la red, cambie su estado a *Aprobada* o *Rechazada*, según sea el caso. Las actualizaciones aprobadas siempre se instalan. Las actualizaciones de estado indefinido solamente se pueden instalar en el Agente de red y en otros componentes de Kaspersky Security Center Cloud Console si lo permite 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 las actualizaciones
- Aprobar y rechazar actualizaciones de software

5. **Configurar la instalación automática de actualizaciones y parches para los componentes de Kaspersky Security Center Cloud Console**

   De manera predeterminada, las actualizaciones y los parches que se descargan para el Agente de red y para los demás componentes de Kaspersky Security Center Cloud Console se instalan automáticamente. Si deja habilitada la opción **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes** en las propiedades del Agente de red, se instalarán todas las actualizaciones que se descarguen en el repositorio (o en los repositorios). Si deshabilita esta opción, los parches de Kaspersky que se descarguen y que tengan el estado *Sin definir* se instalarán únicamente si cambia su estado a *Aprobada*.

   Instrucciones: Habilitar y deshabilitar la instalación automática de actualizaciones y parches para los 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). Recomendamos que, cuando defina la programación de estas tareas, elija la opción **Al descargar nuevas actualizaciones al repositorio**. Con ello tendrá la certeza de que las actualizaciones se instalarán siempre a la primera oportunidad.

   De manera predeterminada, las actualizaciones para las aplicaciones administradas se instalan solo cuando su estado se cambia a *Aprobada*. En el caso de Kaspersky Endpoint Security para Windows, puede modificar los ajustes de actualización en la tarea "Actualizar".

   Si una actualización exige revisar y aceptar los términos del Contrato de licencia de usuario final, es necesario aceptar esos términos para proceder con la instalación. Una vez que se aceptan los términos, la actualización se puede propagar a los dispositivos administrados.

   Instrucciones: Instalación automática de actualizaciones de Kaspersky Endpoint Security en los 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 la actualización de una aplicación de Kaspersky administrada 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 instaló 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 concluir este escenario, puede ocuparse de supervisar el estado de su 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 siempre esté al día, debe proporcionar actualizaciones para los siguientes elementos oportunamente:

- Las bases de datos y los módulos de software de Kaspersky

  Antes de descargar las bases de datos y los módulos de software de Kaspersky, Kaspersky Security Center Cloud Console verifica que haya acceso a los servidores de Kaspersky. Si los servidores DNS configurados en el sistema no permiten acceder a los servidores de Kaspersky, la aplicación utiliza servidores DNS públicos. Esto se hace para garantizar que las bases de datos antivirus se mantengan actualizadas y para que los dispositivos administrados no vean afectado su nivel de seguridad.

- Las aplicaciones de Kaspersky instaladas, incluidas las aplicaciones de seguridad y los componentes de Kaspersky Security Center Cloud Console

  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 y realizar la instalación manualmente.

Existen distintos esquemas para descargar las actualizaciones necesarias y distribuirlas a los dispositivos administrados. La elección de una u otra opción depende de la configuración de la red. Estas son las posibilidades:

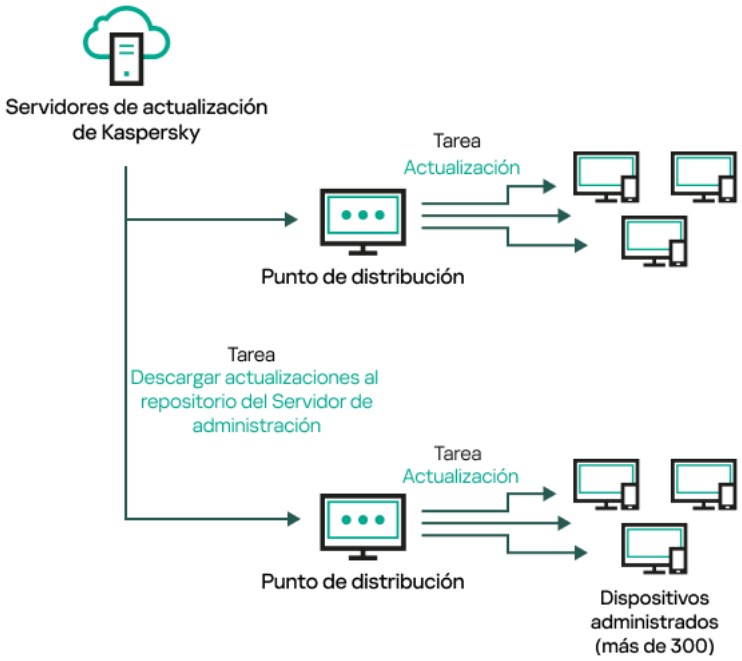
- Utilizar la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*
- Utilizar una carpeta local, una carpeta compartida o un servidor FTP (método manual)
- Hacer que, en los dispositivos administrados, las aplicaciones de seguridad descarguen sus actualizaciones directamente de los servidores de actualizaciones de Kaspersky

Utilizar la tarea Descargar actualizaciones en los repositorios de los puntos de distribución

En este esquema, Kaspersky Security Center Cloud Console descarga las actualizaciones utilizando la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*. Los dispositivos administrados incluidos en el alcance de un punto de distribución descargan las actualizaciones del repositorio de dicho punto de distribución (vea la imagen de más abajo).

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 con la tarea Descargar actualizaciones en los repositorios de los puntos de distribución

Las siguientes actualizaciones se descargan en el repositorio del punto de distribución cuando se completa la tarea *Descargar actualizaciones en los repositorios 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 el administrador aprueba. Las actualizaciones se instalan a través de la tarea "Actualizar" y se pueden configurar en las propiedades de dicha tarea.

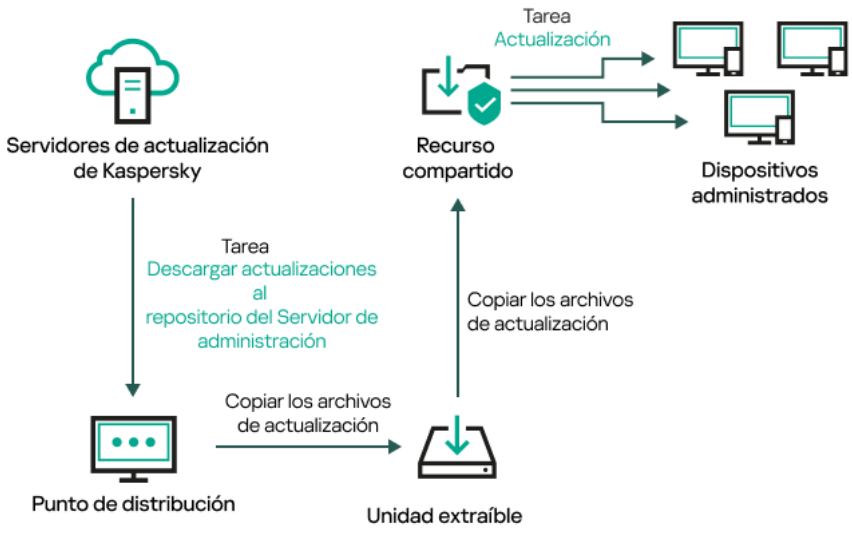
Cada aplicación de Kaspersky le solicita al Servidor de administración las actualizaciones que requiere. El Servidor de administración combina las peticiones y descarga las actualizaciones que las aplicaciones han solicitado (y solo esas actualizaciones) en los repositorios de los puntos de distribución. 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 los 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
- Id. de ejecución de la tarea de descarga

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)

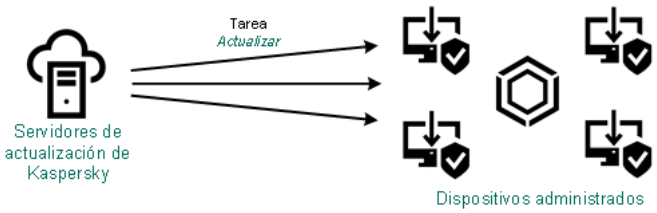
Si sus dispositivos cliente no tienen conexión con un punto de distribución, puede usar una carpeta local o un recurso compartido como origen para actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky. En este caso, deberá copiar las actualizaciones requeridas del repositorio de un punto de distribución a una unidad extraíble, y luego tendrá que copiar esas actualizaciones a la carpeta local o al recurso compartido que haya configurado como origen de actualizaciones en Kaspersky Endpoint Security para Windows (vea la siguiente imagen).



Actualización con una carpeta local, una carpeta compartida o un servidor FTP

Realizar una descarga directa de los servidores de actualizaciones de Kaspersky a Kaspersky Endpoint Security para Windows en los dispositivos administrados

Puede configurar Kaspersky Endpoint Security para Windows en los dispositivos administrados para que la aplicación obtenga sus actualizaciones directamente de los servidores de actualizaciones de Kaspersky (vea la siguiente imagen).



Actualización directa de las aplicaciones de seguridad utilizando los servidores de actualizaciones de Kaspersky

En este esquema, la aplicación de seguridad no utiliza los repositorios que brinda Kaspersky Security Center 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 más información sobre los ajustes pertinentes, 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 los puntos de distribución* para un grupo de administración. Cuando la tarea se ejecute, afectará a los puntos de distribución que formen parte del grupo de administración seleccionado.

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 para 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 los puntos de distribución para un grupo de administración seleccionado:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. Para la aplicación Kaspersky Security Center Cloud Console, en el campo **Tipo de tarea**, seleccione **Descargar actualizaciones en los repositorios de los puntos de distribución**.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Seleccione un botón de opción para elegir el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplicará la tarea.
6. En el paso **Finalizar la creación de la tarea**, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** si desea 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.
7. Haga clic en el botón **Crear**.

   Se crea la tarea y se la agrega a la lista de tareas.
8. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.
9. En la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea, configure los siguientes ajustes:

   - Orígenes de actualizaciones

Los siguientes recursos se pueden utilizar como orígenes de actualizaciones para el punto de distribución:

- Servidores de actualizaciones de Kaspersky

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

  Esta opción está seleccionada de forma predeterminada.

- 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 diff**

  Esta opción habilita la función de descarga de archivos diff.

  Esta opción está deshabilitada de forma predeterminada.

- **Descargar actualizaciones utilizando el esquema anterior**

Cuando Kaspersky Security Center Cloud Console descarga actualizaciones para las bases de datos y los módulos de software, lo hace 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 forma predeterminada.

10. Programe la ejecución de la tarea. De ser necesario, configure los siguientes ajustes:

- **Iniciar tarea**

  Seleccione y configure la programación según la cual se ejecutará la tarea.

  - **Manual** (esta es la opción seleccionada por defecto)

    La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

    Esta opción está seleccionada de forma predeterminada.

  - **Cada N minutos**

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

    De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

  - **Cada N horas**

    La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

    De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

  - **Cada N días**

La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

- **Cada N semanas**

  La tarea se ejecutará periódicamente, a intervalos regulares, en el día de la semana y a la hora que especifique. Cada ejecución estará separada de la anterior por el número de semanas que indique.

  Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta programación no tiene en cuenta los cambios de horario estacionales. La hora de inicio de la tarea se mantendrá sin cambios incluso si el reloj se atrasa o se adelanta una hora debido al horario de verano.

  No recomendamos usar esta programación. Se la ofrece para mantener la compatibilidad con versiones anteriores de Kaspersky Security Center Cloud Console.

  De forma predeterminada, la tarea se iniciará todos los días a la hora actual del sistema.

- **Semanal**

  La tarea se ejecutará cada semana en el día y a la hora que indique.

- **Por días de la semana**

  La tarea se ejecutará periódicamente en los días de la semana y a la hora que indique.

  De manera predeterminada, la tarea se ejecutará todos los viernes a las 18:00:00 p. m.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **Cada mes en los días especificados de semanas seleccionadas**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  De manera predeterminada, no se selecciona ningún día del mes. La hora de inicio predeterminada es a las 18:00.

- **Ante brotes de virus**

La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

- Antivirus para estaciones de trabajo y servidores de archivos
- Antivirus para defensa del perímetro
- Antivirus para sistemas de correo

Por defecto, están seleccionados todos los tipos de aplicaciones.

En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completarse otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. 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 el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

  Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

  Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

  Esta opción está deshabilitada de forma predeterminada.

- **Utilizar retardo aleatorio automático para el inicio de la tarea**

Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

- **Utilizar el retardo aleatorio automático para el inicio de la tarea dentro de un intervalo de**

  Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

  Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

11. Haga clic en el botón **Guardar**.

    La tarea queda creada y configurada.

    Además de los ajustes configurados durante el proceso de creación, la tarea tiene otras propiedades que se pueden modificar.

Cuando se ejecuta la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*, las actualizaciones para las bases de datos y los módulos de software se descargan del origen de actualizaciones y se almacenan en la carpeta compartida. Las actualizaciones descargadas solo serán utilizadas por los puntos de distribución que formen parte del grupo de administración especificado y que no tengan una tarea de descarga de actualizaciones explícitamente definida para ellos.

Configurar los dispositivos administrados para que solo se actualicen mediante los puntos de distribución

Los dispositivos administrados pueden obtener actualizaciones para las bases de datos, los módulos de software y las aplicaciones de Kaspersky de distintas fuentes: de los servidores de actualizaciones, de los puntos de distribución o de una carpeta local o de red. Los puntos de distribución pueden definirse como único origen de actualizaciones posible.

Para que los dispositivos administrados reciban sus actualizaciones únicamente de 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 interruptor **Distribuir archivos solo a través de los puntos de distribución**.

5. Bloquee (🔒) el interruptor.

6. Haga clic en el botón **Guardar**.

La directiva se aplicará a los dispositivos seleccionados. Estos pasarán a recibir sus actualizaciones únicamente de los puntos de distribución.

Habilitar y deshabilitar la instalación automática de actualizaciones y parches para los componentes de Kaspersky Security Center Cloud Console

De manera predeterminada, cuando el Agente de red se instala en un dispositivo, se habilita la instalación automática de actualizaciones y parches para los componentes de Kaspersky Security Center Cloud Console. Si quiere deshabilitar esta característica, puede hacerlo al instalar el Agente de red o en cualquier otro momento a través de una directiva.

Para deshabilitar la instalación automática de actualizaciones y parches para los componentes de Kaspersky Security Center Cloud Console al instalar el Agente de red en un dispositivo (si la instalación se realiza en forma local):

1. Inicie la instalación del Agente de red de manera local 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.

El Agente de red se instalará en el dispositivo. La autoinstalación de actualizaciones y parches para los componentes de Kaspersky Security Center Cloud Console quedará deshabilitada. Si desea habilitar la autoinstalación de actualizaciones y parches más adelante, podrá hacerlo a través de una directiva.

Para deshabilitar la instalación automática de actualizaciones y parches para los componentes de Kaspersky Security Center Cloud Console al instalar el Agente de red en un dispositivo (si la instalación se realiza con un paquete de instalación):

1. En el menú principal, vaya a **Operaciones → Repositorios → Paquetes de instalación**.

2. Haga clic en el paquete **Agente de red de Kaspersky Security Center <número de versión>**.

3. En la ventana de propiedades, seleccione la pestaña **Configuración**.

4. Desactive el interruptor **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes**.

El Agente de red se instalará desde el paquete. La autoinstalación de actualizaciones y parches para los componentes de Kaspersky Security Center Cloud Console quedará deshabilitada. Si desea habilitar la autoinstalación de actualizaciones y parches más adelante, podrá hacerlo a través de una directiva.

Si activó (o desactivó) la casilla del paso 4 al instalar el Agente de red en el dispositivo, puede habilitar (o deshabilitar) la actualización automática posteriormente a través de la directiva del Agente de red.

Para habilitar o deshabilitar la instalación automática de actualizaciones y parches para los componentes de Kaspersky Security Center Cloud Console mediante la directiva del Agente de red:

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 las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes** para habilitar o deshabilitar, respectivamente, la instalación automática de actualizaciones y parches.
5. Asegúrese de definir (**aplicar**) el atributo de bloqueo (🔒) para este interruptor.

La directiva se aplicará a los dispositivos seleccionados. La autoinstalación de actualizaciones y parches para los componentes de Kaspersky Security Center Cloud Console quedará habilitada o deshabilitada, según corresponda, en esos dispositivos.

Instalación automática de actualizaciones para Kaspersky Endpoint Security para Windows

Puede hacer que las bases de datos y los módulos de software de Kaspersky Endpoint Security para Windows se actualicen automáticamente en los dispositivos cliente.

Para que las actualizaciones de Kaspersky Endpoint Security para Windows se descarguen y se instalen automáticamente en los dispositivos cliente, haga lo siguiente:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en el botón **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. Busque la aplicación Kaspersky Endpoint Security para Windows y seleccione **Actualizar** como subtipo de tarea.
4. Escriba un nombre para la tarea que está creando. El nombre de la tarea no puede tener más de 100 caracteres ni debe incluir caracteres especiales ("*<>?\:|).
5. Elija el alcance de la tarea.
6. Elija el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplicará la tarea.
7. En el paso **Finalizar la creación de la tarea**, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** si desea 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.
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**. Utilice esta pestaña para determinar cómo el dispositivo recibirá sus actualizaciones cuando haya conexión entre el mismo y el Servidor de administración.

    - **Modo móvil**. Utilice esta pestaña para determinar cómo el dispositivo recibirá sus actualizaciones cuando no haya conexión entre el mismo y Kaspersky Security Center Cloud Console (por ejemplo, cuando el dispositivo no esté 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. De ser necesario, utilice los botones **Subir** y **Bajar** para cambiar el orden de los orígenes en la lista. 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.

    Si utiliza Kaspersky Security Center Cloud Console como origen de actualizaciones, tenga en cuenta que las actualizaciones se descargarán de los repositorios de los puntos de distribución, no del repositorio del Servidor de administración. Asegúrese de que haya puntos de distribución designados y no olvide crear la tarea *Descargar actualizaciones en los repositorios de los 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 estableció 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 la política de privacidad. Cuando este sea el caso, la aplicación esperará a que el usuario acepte los términos de estos documentos y luego instalará las actualizaciones.

13. Marque la casilla **Copiar actualizaciones a la siguiente carpeta** para que la aplicación guarde las actualizaciones descargadas en una carpeta. A continuación, elija la carpeta de destino.

14. Defina una programación para la tarea. Recomendamos seleccionar la opción **Al descargar nuevas actualizaciones al repositorio** de manera que las actualizaciones se instalen sin demora.

15. Haga clic en **Guardar**.

    Cuando la tarea **Actualizar** está en ejecución, la aplicación envía solicitudes a los servidores de actualizaciones de Kaspersky.

Algunas actualizaciones requieren que estén instaladas las últimas versiones de los complementos de administración.

Acerca de los estados de las actualizaciones

El *estado* de una actualización es un atributo que determina si esa actualización debe instalarse o no en un dispositivo de la red.

Las actualizaciones pueden tener los siguientes estados:

- *Sin definir*

  De forma predeterminada, las actualizaciones de software descargadas tienen el estado *Sin definir*. Las actualizaciones de estado indefinido solamente se pueden instalar en el Agente de red y en otros componentes de Kaspersky Security Center Cloud Console si lo permite 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 el siguiente software:

- El Agente de red y otros componentes de Kaspersky Security Center Cloud Console

  De manera predeterminada, las actualizaciones y los parches que se descargan para los componentes de Kaspersky Security Center Cloud Console se instalan automáticamente. Si deja habilitada la opción **Instalar automáticamente las actualizaciones y parches de estado Sin definir que estén disponibles para los componentes** en las propiedades del Agente de red, se instalarán todas las actualizaciones que se descarguen en el repositorio (o en los repositorios). Si deshabilita esta opción, los parches de Kaspersky que se descarguen y que tengan el estado *Sin definir* se instalarán únicamente si cambia su estado a *Aprobada*.

  Las actualizaciones para los componentes de Kaspersky Security Center Cloud Console no pueden desinstalarse, ni siquiera si se les asigna el estado *Rechazada*.

- Las aplicaciones de seguridad de Kaspersky

  De manera predeterminada, las actualizaciones para las aplicaciones administradas se instalan solo cuando su estado se cambia a *Aprobada*. Si rechaza una actualización que ya se había instalado para una aplicación de seguridad, Kaspersky Security Center Cloud Console intentará desinstalar esa 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 y realizar la instalación manualmente.

Para aprobar o rechazar una o más actualizaciones:

1. En el menú principal, vaya a **Operaciones → Aplicaciones de Kaspersky → Actualizaciones sin interrupciones**.

   Se mostrará una lista con las actualizaciones disponibles.

   Las actualizaciones para las aplicaciones administradas pueden requerir que la versión de Kaspersky Security Center instalada sea posterior a una versión en particular. Si está utilizando una versión anterior a la necesaria, podrá ver estas actualizaciones, pero no las podrá aprobar. Tampoco podrá crear paquetes de instalación a partir de esas actualizaciones hasta que actualice Kaspersky Security Center. Si intenta hacerlo, se le pedirá que actualice su copia de Kaspersky Security Center a la versión mínima requerida.

2. Si es necesario, acepte el EULA haciendo clic en el botón **Ver y aceptar los 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 asigne el estado *Aprobada* se pondrán en una cola para ser instaladas.

Las actualizaciones a las que les asigne el estado *Rechazada* se desinstalarán (si tal acción es posible) de todos los dispositivos en los que estén instaladas. Estas actualizaciones no se instalarán en otros dispositivos en el futuro.

Existen actualizaciones para las aplicaciones de Kaspersky que no se pueden desinstalar. Si configura el estado *Rechazado* 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 eliminarán 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 archivo diff ocupa menos espacio que una copia completa de la base de datos o el módulo de software, por lo que su uso permite reducir el volumen de tráfico en la red de la empresa. Si la función de *descarga de archivos diff* está habilitada en un punto de distribución, los archivos diff se guardan en este punto de distribución. Como resultado, los dispositivos que obtengan sus actualizaciones de dicho punto de distribución podrán usar los archivos diff guardados para actualizar sus bases de datos y módulos de software.

Para optimizar el uso de los archivos diff, recomendamos que sincronice la frecuencia de actualización de los dispositivos con la frecuencia de actualización del punto de distribución del que los dispositivos tomen sus actualizaciones. No obstante, podrá ver una merma en el volumen de tráfico incluso si los dispositivos se actualizan con bastante menos frecuencia que el punto de distribución del que toman las actualizaciones.

Los puntos de distribución no utilizan la multidifusión IP para la distribución automática de archivos diff.

Para habilitar la función de descarga de archivos diff, haga lo siguiente:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución* para abrir las propiedades de la tarea.
3. En la pestaña **Configuración de la aplicación**, habilite la opción **Descargar archivos diff**.
4. Haga clic en el botón **Guardar**.

   La función de descarga de archivos diff queda habilitada. Cada vez que se ejecute la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*, además de los archivos de actualización, se descargarán los archivos diff de esas actualizaciones.

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 de los repositorios de los puntos de distribución.

Si necesita actualizar las bases de datos y los módulos de software en un dispositivo (o en un grupo de dispositivos) que no está conectado a un punto de distribución o que no tiene acceso a Internet, deberá usar un origen de actualizaciones alternativo, como una carpeta local o un servidor FTP. 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 de las siguientes fuentes:

- Punto de distribución.

Para que el repositorio de un punto de distribución contenga las actualizaciones necesarias para la aplicación de seguridad de un dispositivo sin conexión, esa misma aplicación debe estar instalada en al menos un dispositivo administrado que tenga acceso al punto de distribución y esté incluido en su alcance. Esta segunda copia de la aplicación debe estar configurada para obtener sus actualizaciones del repositorio del punto de distribución mediante la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*.

- Cualquier dispositivo que tenga instalada la misma aplicación de seguridad y que obtenga sus actualizaciones del repositorio de un punto de distribución o directamente de los servidores de actualizaciones de Kaspersky.

A continuación, se describe un método para actualizar las bases de datos y los módulos de una aplicación con archivos copiados del repositorio de un punto de distribución.

Para actualizar las bases de datos y los módulos de software de Kaspersky en dispositivos sin conexión:

1. Conecte una unidad extraíble al dispositivo que actúa como punto de distribución.
2. Copie los archivos de las actualizaciones a la unidad extraíble.

   De forma predeterminada, las actualizaciones se encuentran en la carpeta %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.

Actualizar las bases de datos de Kaspersky Security for Windows Server

Si ha instalado Kaspersky Security for Windows Server en sus dispositivos administrados, posiblemente quiera iniciar la tarea "Protección de archivos en tiempo real" de esa aplicación. Para que esta tarea funcione correctamente, se requieren bases de datos que no vienen incluidas en la aplicación. Las bases de datos necesarias se descargan en el dispositivo administrado una vez que se completa la tarea *Descargar actualizaciones en los repositorios de los 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 de la aplicación se descarguen y estén actualizadas. De lo contrario, la tarea podría no funcionar correctamente.

Para asegurarse de que las bases de datos de Kaspersky Security for Windows Server estén actualizadas, haga lo siguiente:

1. Verifique que la tarea *Descargar actualizaciones en los repositorios de los 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, habilite la opción de inicio **Al iniciar la aplicación**. A continuación, reinicie el dispositivo administrado.

- En la configuración de la tarea "Protección de archivos en tiempo real", defina manualmente la hora de inicio que considere conveniente.

La tarea "Protección de archivos en tiempo real" de Kaspersky Security for Windows Server queda lista para funcionar correctamente.

Administración de aplicaciones de terceros en dispositivos cliente

En esta sección, se describen las características de Kaspersky Security Center Cloud Console que permiten administrar las aplicaciones de terceros instaladas en los dispositivos cliente.

Limitaciones de la característica Administración de vulnerabilidades y parches

La característica Administración de vulnerabilidades y parches está sujeta a ciertas limitaciones, que varían según la licencia y el modo de funcionamiento de Kaspersky Security Center Cloud Console.

Las siguientes licencias no son compatibles con la característica Administración de vulnerabilidades y parches:

- Kaspersky Endpoint Security for Business Select
- Kaspersky Hybrid Cloud Security

Las siguientes licencias son compatibles con la característica 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

En la siguiente tabla, se comparan las limitaciones que rigen cuando Kaspersky Security Center Cloud Console se utiliza en modo de prueba, con licencias que no son compatibles con Administración de vulnerabilidades y parches y con licencias que sí son compatibles con esta característica.

Limitaciones de la característica Administración de vulnerabilidades y parches

Limitación	Modo de prueba	Modo comercial, licencias incompatibles con Administración de vulnerabilidades y parches	Modo comercial, licencias compatibles con Administración de vulnerabilidades y parches
Número máximo de tareas *Instalar actualizaciones de Windows Update* o *Reparar vulnerabilidades*	4	4	0 (no es posible crear nuevas tareas de estos tipos)
Número máximo de tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades*	2	No disponible	4
Número máximo de reglas para todas las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades*	10	No disponible	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 disponible	1000
Cantidad máxima de actualizaciones de software que se pueden agregar manualmente a una tarea, en todos los servidores, incluidos los virtuales	500	1000	1000
Cantidad máxima de vulnerabilidades de software que se pueden agregar manualmente a una tarea, en todos los servidores, incluidos los virtuales	500	1000	1000

Características Administración de vulnerabilidades y parches disponibles en modo comercial, en modo de prueba y con distintas opciones de licencia

La disponibilidad de funciones de Administración de vulnerabilidades y parches en Kaspersky Security Center Cloud Console varía según el modo en que se utiliza la solución (modo comercial o modo de prueba) y según la opción de licencia que se ha seleccionado. Utilice la siguiente tabla para verificar cuáles son las funciones de Administración de vulnerabilidades y parches a las que tiene acceso.

Disponibilidad de las características Administración de vulnerabilidades y parches

Característica 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
Reparar vulnerabilidades manualmente en las aplicaciones de Microsoft de los dispositivos con Windows administrados Crear la tarea *Reparar vulnerabilidades*	✓	✓	—
Instalar actualizaciones manualmente en las aplicaciones de Microsoft de los dispositivos con Windows administrados Instalación de actualizaciones de software de terceros a través de la tarea *Instalar actualizaciones de Windows Update*	—	✓	✓
Utilizar reglas para instalar actualizaciones en el software de terceros y para reparar vulnerabilidades en el software de terceros automáticamente 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 solamente puede actualizar software de terceros de la versión instalada 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 **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En el paso **Configuración de tarea nueva** del asistente, especifique estos ajustes:

   a. En la lista desplegable **Aplicación**, seleccione **Kaspersky Security Center Cloud Console**.

   b. En el campo **Tipo de tarea**, seleccione **Instalar actualizaciones requeridas y reparar vulnerabilidades**.

4. En el paso **Alcance de la tarea** del asistente, seleccione la opción **Dispositivos administrados**.

5. En el paso del asistente **Elija las reglas de instalación de actualizaciones**, haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

6. En el paso del asistente **Seleccionar tipo de regla**, seleccione **Regla para actualizaciones de terceros**.

7. En el paso del asistente **Criterios generales**, seleccione la opción **Instalar todas las actualizaciones (excepto las rechazadas)** y, luego, haga clic en **Siguiente**.

Se muestra la lista de software de terceros.

Actualizaciones para el software de terceros

Kaspersky Security Center Cloud Console permite administrar las actualizaciones del software de terceros instalado en los dispositivos administrados. También permite reparar, mediante la instalación de las actualizaciones pertinentes, las vulnerabilidades que se detectan en las aplicaciones de Microsoft y en los productos de otros desarrolladores.

Kaspersky Security Center Cloud Console utiliza la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para buscar actualizaciones. Cuando se completa esta tarea, el Servidor de administración recibe listas en las que se detallan las vulnerabilidades detectadas y las actualizaciones requeridas para el software de terceros con el que cuentan los dispositivos indicados en las propiedades de la tarea. Tras ver la información de las actualizaciones disponibles, puede instalarlas en los dispositivos.

Para actualizar algunas aplicaciones, Kaspersky Security Center Cloud Console elimina la versión antigua de la aplicación e instala la versión nueva.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedírsele al usuario que la cierre.

Por seguridad, cada actualización de software de terceros que se instala con la función Administración de vulnerabilidades y parches se somete a un análisis antimalware automático con las tecnologías de Kaspersky Estas tecnologías revisan automáticamente los archivos utilizando técnicas de análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno de pruebas y aprendizaje automático, entre otras.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. 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 instalar 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. Cada vez que se descargan metadatos de nuevas actualizaciones en el repositorio del Servidor de administración, Kaspersky Security Center Cloud Console verifica si las actualizaciones cumplen con los criterios especificados en las reglas de actualización. Las actualizaciones nuevas que cumplen con los criterios se descargan e instalan en forma automática cuando la tarea se ejecuta nuevamente.

- La tarea *Instalar actualizaciones de Windows Update*

  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. Si necesita instalar nuevas actualizaciones más adelante, agregue esas actualizaciones a la lista de actualizaciones de la tarea existente o, si lo prefiere, cree una nueva 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 bajo la cual utiliza Kaspersky Security Center Cloud Console y del modo en el que Kaspersky Security Center Cloud Console está funcionando.

Procedimiento: Actualización de software de terceros

En esta sección, se describe un escenario para actualizar el software de terceros instalado en los dispositivos cliente. El término "software de terceros" comprende aplicaciones desarrolladas por Microsoft y por otros proveedores de software. Las actualizaciones para las aplicaciones de Microsoft se obtienen a través del servicio Windows Update.

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 listas con las vulnerabilidades detectadas y las actualizaciones requeridas para el software de terceros que se encuentra instalado en los dispositivos indicados en las propiedades de la tarea.

La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente al utilizar el asistente de inicio rápido del Servidor de administración. Si no ejecutó el asistente de inicio rápido, hágalo ahora o cree la tarea.

Instrucciones:

- Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas
- Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

2. **Analizar la lista de actualizaciones encontradas**

Abra la lista **Actualizaciones de software** y decida qué actualizaciones se instalarán. Para obtener información detallada sobre una actualización, haga clic en el nombre de la misma en la lista. Puede acceder a estadísticas sobre el estado de instalación de cada actualización en los dispositivos administrados. Puede ver, por ejemplo, en cuántos dispositivos no se ha instalado una actualización de la lista, en cuántos está pendiente de instalarse y en cuántos se intentó instalarla, pero, por algún motivo, la instalación no se completó.

Instrucciones: Ver información sobre las actualizaciones disponibles para el software de terceros

3. **Configurar la instalación de actualizaciones**

Una vez que Kaspersky Security Center Cloud Console cuenta con la lista de actualizaciones para el software de terceros, utilice una de dos tareas para instalarlas en los dispositivos cliente: la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Instalar actualizaciones de Windows Update*. Cree una de estas tareas. Puede crearlas desde la pestaña **Tareas** o a través de la lista **Actualizaciones de software**.

La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se utiliza para instalar actualizaciones para aplicaciones de Microsoft (incluidas las actualizaciones que proporciona el servicio Windows Update) y actualizaciones para software de otros proveedores.

La tarea *Instalar actualizaciones de Windows Update* puede usarse únicamente 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 bajo la cual utiliza Kaspersky Security Center Cloud Console y del modo en el que Kaspersky Security Center Cloud Console está funcionando.

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 creó la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede programarla para que se ejecute con igual o menor frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Al programar la tarea *Instalar actualizaciones de Windows Update*, tenga en cuenta que deberá definir la lista de actualizaciones a instalar cada vez que la tarea vaya a iniciarse.

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: Ajustes generales de las tareas

5. **Aprobar y rechazar actualizaciones de software (opcional)**

Si creó la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede especificar reglas para la instalación de actualizaciones en las propiedades de la tarea. Si creó la tarea *Instalar actualizaciones de Windows Update*, omita este paso.

Para cada regla, puede definir las actualizaciones que se instalarán según el estado de la actualización (*Sin definir*, *Aprobada* o *Rechazada*). Si crea una tarea específica para sus servidores, por ejemplo, podría definir una regla que únicamente permita la instalación de actualizaciones que provengan de Windows Update y que tengan el estado *Aprobada*. Tras ello, podría asignar manualmente el estado *Aprobada* a las actualizaciones que desee instalar. Las actualizaciones de Windows Update que tengan el estado *Sin definir* o el estado *Rechazada* no se instalarán en los servidores especificados en la tarea.

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 la tarea de instalación de actualizaciones**

   Inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Instalar actualizaciones de Windows Update*. Al hacerlo, se descargarán las actualizaciones y se las instalará en los dispositivos administrados. Cuando se complete la tarea ejecutada, verifique que su estado en la lista de tareas sea *Completada correctamente*.

   Instrucciones: Inicio de una tarea de forma manual

7. **Crear el informe sobre los resultados de la instalación de actualizaciones de software de terceros (opcional)**

   Para asegurarse de que la tarea se haya creado correctamente y comprobar que las actualizaciones estén instaladas, cree el informe llamado **Informe sobre los resultados de la instalación de actualizaciones de software de terceros**. En él encontrará estadísticas detalladas sobre la instalación de las actualizaciones.

   Instrucciones: Generar y ver un informe

Instalación de actualizaciones para software de terceros

Para instalar actualizaciones para software de terceros en sus dispositivos administrados, debe crear y ejecutar alguna de las siguientes tareas:

- *Instalar actualizaciones requeridas y reparar vulnerabilidades*

  Utilice esta tarea para instalar actualizaciones de Windows Update proporcionadas por Microsoft o actualizaciones para productos de otros proveedores.

- *Instalar actualizaciones de Windows Update*

  Utilice esta tarea si solo necesita instalar actualizaciones de Windows Update.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia bajo la cual utiliza Kaspersky Security Center Cloud Console y del modo en el que Kaspersky Security Center Cloud Console está funcionando.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

Como alternativa, para crear una tarea que instale las actualizaciones requeridas, puede optar por estos métodos:

- Abra la lista de actualizaciones y elija las actualizaciones que se deban instalar.

Como resultado, se creará una nueva tarea para instalar las actualizaciones seleccionadas. Si lo prefiere, puede agregar las actualizaciones seleccionadas a una tarea existente.

- Utilice el Asistente de instalación de actualizaciones.

  La disponibilidad del Asistente de instalación de actualizaciones depende del modo de Kaspersky Security Center Cloud Console y de la licencia que se está utilizando.

  El asistente simplifica la creación y configuración de tareas de instalación de actualizaciones. También evita que se creen tareas redundantes, que tengan 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 de actualizaciones general, en el menú principal, vaya a **Operaciones → Administración de parches → Actualizaciones de software**.
   - Para abrir la lista de actualizaciones de un dispositivo administrado, en el menú principal, vaya a **Activos (dispositivos) → Dispositivos administrados → <nombre del dispositivo> → Avanzado → Actualizaciones disponibles**.
   - Para abrir la lista de actualizaciones para una aplicación específica, en el menú principal, vaya a **Operaciones → Aplicaciones de terceros → Registro de aplicaciones → <nombre de la aplicación> → Actualizaciones disponibles**.

   Se mostrará una lista con las actualizaciones disponibles.

2. Marque las casillas de verificación ubicadas junto a las actualizaciones que desee instalar.

3. Haga clic en el botón **Instalar actualizaciones**.

   Para instalar algunas actualizaciones de software, deberá aceptar el contrato de licencia de usuario final (EULA). Si rechaza el EULA, no se instalará la actualización de software correspondiente.

4. Seleccione una de las siguientes opciones:

   - **Nueva tarea**

     Se inicia el Asistente para crear nueva tarea. Dependiendo del modo de Kaspersky Security Center Cloud Console y de la licencia que esté utilizando, estará preseleccionada la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Instalar actualizaciones de Windows Update*. Siga los pasos del asistente para completar la creación de la tarea.

   - **Instalar actualización (agregar regla a la tarea especificada)**

     Seleccione una tarea a la que desee agregar las actualizaciones seleccionadas. Puede elegir una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o una tarea *Instalar actualizaciones de Windows Update*. Si selecciona una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, se agregará automáticamente a esa tarea una nueva regla para instalar las actualizaciones seleccionadas. Si selecciona una tarea *Instalar actualizaciones de Windows Update*, las actualizaciones seleccionadas se agregarán a las propiedades de la tarea.

     Se abrirá la ventana de propiedades de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

Si optó por crear una tarea, se la creará y se la agregará a la lista de tareas disponible en **Activos (dispositivos)** → **Tareas**. Si eligió agregar las actualizaciones a una tarea existente, se agregarán las actualizaciones a las propiedades de la tarea que haya seleccionado.

Para instalar las actualizaciones para el software de terceros, inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Instalar actualizaciones de Windows Update*. Puede iniciar cualquiera de estas dos tareas de forma manual o, si lo prefiere, puede configurar una programación en las propiedades de la tarea que desee iniciar. Si elige configurar una programación, asegúrese de que la tarea de instalación de actualizaciones se ejecute luego de que finalice la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

Instalación de actualizaciones de software de terceros mediante el Asistente de instalación de actualizaciones

La disponibilidad de esta función depende del modo de Kaspersky Security Center Cloud Console y de la licencia que se está utilizando.

Para crear una tarea para instalar actualizaciones de software de terceros con el Asistente de instalación de actualizaciones:

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Actualizaciones de software**.

   Se mostrará una lista con las actualizaciones disponibles.

2. Marque la casilla ubicada junto a la actualización que desee instalar.

3. Haga clic en el botón **Ejecutar el Asistente de instalación de actualizaciones**.

   Se iniciará el Asistente de instalación de actualizaciones. En la página **Seleccione una tarea de instalación de actualizaciones**, verá una lista con las tareas existentes de los siguientes tipos:

   - *Instalar actualizaciones requeridas y reparar vulnerabilidades*
   - *Instalar actualizaciones de Windows Update*
   - *Reparar vulnerabilidades*

   No puede modificar las tareas de los dos últimos tipos para instalar nuevas actualizaciones. Para instalar nuevas actualizaciones, solo puede utilizar las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

4. Si desea que el asistente solamente le muestre las tareas que permitan instalar la actualización seleccionada, habilite la opción **Mostrar solo las tareas que permitan instalar esta actualización**.

5. Elija lo que desea hacer:

   - Para iniciar una tarea, marque la casilla ubicada junto al nombre de la tarea en cuestión y haga clic en el botón **Iniciar**.
   - Para agregar una nueva regla a una tarea existente, haga lo siguiente:

     a. Marque la casilla ubicada junto al nombre de la tarea pertinente y haga clic en el botón **Agregar regla**.

     b. En la página que se abrirá, configure la nueva regla:

     - Regla de instalación para actualizaciones de este nivel de importancia

Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

Esta opción está deshabilitada de forma predeterminada.

- Regla de instalación para actualizaciones de este nivel de importancia conforme a MSRC (disponible solo para actualizaciones de Windows Update)

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción (que solo está disponible para actualizaciones de Windows Update) está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

  Esta opción está deshabilitada de forma predeterminada.

- Regla de instalación para actualizaciones de este proveedor (disponible solo para actualizaciones de aplicaciones de terceros)

  Esta opción solo está disponible para actualizaciones de aplicaciones de terceros. Kaspersky Security Center Cloud Console únicamente instalará aquellas actualizaciones que estén vinculadas a las aplicaciones del mismo proveedor al que corresponda la actualización seleccionada. No se instalarán actualizaciones rechazadas ni actualizaciones para software de otros proveedores.

  Esta opción está deshabilitada de forma predeterminada.

- **Regla de instalación para actualizaciones del tipo**
- **Regla de instalación para la actualización seleccionada**
- Aprobar actualizaciones seleccionadas

  Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

  Esta opción está deshabilitada de forma predeterminada.

- Instalar automáticamente todas las actualizaciones de software que antecedan a las seleccionadas y se requieran para instalarlas

Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

Esta opción está activada de forma predeterminada.

c. Haga clic en el botón **Agregar**.

- Para crear una tarea:

a. Haga clic en el botón **Nueva tarea**.

b. En la página que se abrirá, configure la nueva regla:

- Regla de instalación para actualizaciones de este nivel de importancia

Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

Esta opción está deshabilitada de forma predeterminada.

- Regla de instalación para actualizaciones de este nivel de importancia conforme a MSRC (disponible solo para actualizaciones de Windows Update)

Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

Si esta opción (que solo está disponible para actualizaciones de Windows Update) está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

Esta opción está deshabilitada de forma predeterminada.

- Regla de instalación para actualizaciones de este proveedor (disponible solo para actualizaciones de aplicaciones de terceros)

Esta opción solo está disponible para actualizaciones de aplicaciones de terceros. Kaspersky Security Center Cloud Console únicamente instalará aquellas actualizaciones que estén vinculadas a las aplicaciones del mismo proveedor al que corresponda la actualización seleccionada. No se instalarán actualizaciones rechazadas ni actualizaciones para software de otros proveedores.

Esta opción está deshabilitada de forma predeterminada.

- **Regla de instalación para actualizaciones del tipo**
- **Regla de instalación para la actualización seleccionada**
- **Aprobar actualizaciones seleccionadas**

  Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

  Esta opción está deshabilitada de forma predeterminada.

- **Instalar automáticamente todas las actualizaciones de software que antecedan a las seleccionadas y se requieran para instalarlas**

  Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

  Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

  A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

  Esta opción está activada de forma predeterminada.

c. Haga clic en el botón **Agregar**.

Si eligió iniciar una tarea, puede cerrar el asistente. La tarea se completará en segundo plano. No se requieren más acciones.

Si optó por agregar una regla a una tarea existente, se abrirá la ventana de propiedades de la tarea. Encontrará la nueva regla en las propiedades de la tarea. Si lo desea, vea y modifique la regla u otros ajustes de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

Si eligió crear una tarea, continúe creándola en el Asistente para crear nueva tarea. La nueva regla que agregó en el Asistente de instalación de actualizaciones se mostrará en el Asistente para crear nueva tarea. Cuando finalice el Asistente para crear nueva tarea, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se agregará a la lista de tareas.

Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas

Mediante la tarea Buscar vulnerabilidades y actualizaciones requeridas, Kaspersky Security Center Cloud Console recibe listas en las que se enumeran las vulnerabilidades detectadas y las actualizaciones que se requieren para el software de terceros instalado en los dispositivos administrados.

La tarea Buscar vulnerabilidades y actualizaciones requeridas se crea automáticamente cuando se ejecuta el asistente de inicio rápido. Si no ha ejecutado este asistente, puede crear la tarea de forma manual.

Para crear una tarea del tipo Buscar vulnerabilidades y actualizaciones requeridas:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. Para la aplicación 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 la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.
7. Haga clic en el botón **Crear**.

   Se crea la tarea y se la agrega a la lista de tareas.
8. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.
9. En la ventana de propiedades de la tarea, configure los ajustes generales de la tarea.
10. En la pestaña **Configuración de la aplicación**, defina los siguientes ajustes:

    - **Buscar vulnerabilidades y actualizaciones catalogadas por Microsoft**

      Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center Cloud Console utilizará la información sobre las actualizaciones de Microsoft aplicables y disponibles que le brinde el origen de actualizaciones de Microsoft.

      Podría deshabilitar esta opción si, por ejemplo, ha creado tareas diferentes (con configuraciones diferentes) para las actualizaciones de Microsoft y para las actualizaciones de aplicaciones de terceros.

      Esta opción está activada de forma predeterminada.

      La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

    - **Conectarse al servidor de actualizaciones para actualizar los datos**

El Agente de Windows Update del dispositivo administrado se conectará al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como orígenes de actualizaciones de Microsoft:

- El Servidor de administración de Kaspersky Security Center Cloud Console (vea los ajustes de la directiva del Agente de red)
- Un servidor Windows Server con Microsoft Windows Server Update Services (WSUS) que se encuentre instalado en la red de su organización
- Los servidores de actualizaciones de Microsoft

Cuando esta opción está habilitada, el Agente de Windows Update del dispositivo administrado se conecta al origen de actualizaciones de Microsoft para obtener información actualizada sobre las actualizaciones de Microsoft Windows aplicables.

Cuando esta opción está deshabilitada, el Agente de actualización de Windows del dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que el origen de actualizaciones brindó en un momento anterior.

Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Podría deshabilitar esta opción si ha configurado un esquema de conexión periódica a este origen en otra tarea o en la sección **Actualizaciones y vulnerabilidades de software** de las propiedades de la directiva del Agente de red. Si no quiere deshabilitar esta opción, para intentar que el Servidor de administración no se sobrecargue, modifique la programación de la tarea para que se la inicie en un punto aleatorio de un intervalo de 360 minutos.

Esta opción está activada de forma predeterminada.

El modo de obtener las actualizaciones deriva de combinar las siguientes opciones de configuración de la directiva del Agente de red:

- El Agente de Windows Update en un dispositivo administrado se conecta al Servidor de actualizaciones para obtener actualizaciones solo si la opción **Conectarse al servidor de actualizaciones para actualizar los datos** está activada en las propiedades de la tarea *Buscar vulnerabilidades y actualizaciones requeridas* y la opción de **Modo de búsqueda de Windows Update** está configurada como **Activo** en la configuración de la directiva del Agente de red.
- Si no necesita el Agente de red para iniciar una conexión al origen de actualizaciones de Microsoft Windows ni para descargar actualizaciones al realizar la tarea *Análisis de vulnerabilidades*, puede seleccionar la opción **Pasivo** en **Modo de búsqueda de Windows Update**, pero la opción **Conectarse al servidor de actualizaciones para actualizar los datos** debe permanecer habilitada. Así podrá ahorrar recursos y usar las actualizaciones de Windows antes recibidas para analizar las vulnerabilidades. Puede usar el modo pasivo si configura la recepción de actualizaciones de Microsoft Windows de otra manera. Si la recepción de actualizaciones de Microsoft Windows no está configurada de otra manera, no seleccione la opción **Pasivo** en **Modo de búsqueda de Windows Update** porque, en este caso, nunca recibirá información sobre las actualizaciones.
- Independientemente del estado de la opción **Conectarse al servidor de actualizaciones para actualizar los datos** (activada o desactivada), si la opción **Deshabilitado** está marcada en **Modo de búsqueda de Windows Update**, Kaspersky Security Center Cloud Console no solicita ninguna información sobre actualizaciones.

- Buscar vulnerabilidades y actualizaciones catalogadas por Kaspersky para software de terceros

Si esta opción está habilitada, Kaspersky Security Center Cloud Console Cloud Console buscará vulnerabilidades y actualizaciones para las aplicaciones de terceros (aplicaciones creadas por proveedores de software que no sean ni Kaspersky ni Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky determina el alcance de la lista de aplicaciones de terceros compatibles.

Si esta opción está deshabilitada, Kaspersky Security Center Cloud Console no buscará vulnerabilidades ni actualizaciones para aplicaciones de terceros. Puede que quiera deshabilitar esta opción si utiliza tareas diferentes, con configuraciones diferentes, para las actualizaciones de Microsoft Windows y para las actualizaciones de aplicaciones de terceros.

Esta opción está activada de forma predeterminada.

- **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**

  Las carpetas en las que Kaspersky Security Center Cloud Console buscará aplicaciones de terceros que deban actualizarse o que tengan vulnerabilidades para reparar. Puede utilizar variables del sistema.

  Especifique las carpetas en las que se instalan las aplicaciones. De manera predeterminada, la lista está vacía.

- **Habilitar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red guardará datos de seguimiento incluso si la función de seguimiento se ha deshabilitado 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. Puede usar la utilidad de diagnóstico remoto para acceder a estos archivos, descargarlos y eliminarlos.

  Si esta función está deshabilitada, el Agente de red determinará si debe o no guardar información de seguimiento guiándose por 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 forma predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

11. Haga clic en el botón **Guardar**.

La tarea queda creada y configurada.

Si 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 catalogadas por Microsoft**

  Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center Cloud Console utilizará la información sobre las actualizaciones de Microsoft aplicables y disponibles que le brinde el origen de actualizaciones de Microsoft.

  Podría deshabilitar esta opción si, por ejemplo, ha creado tareas diferentes (con configuraciones diferentes) para las actualizaciones de Microsoft y para las actualizaciones de aplicaciones de terceros.

  Esta opción está activada de forma predeterminada.

  La información sobre las actualizaciones opcionales de Microsoft Windows no se envía al Servidor de administración.

- **Conectarse al servidor de actualizaciones para actualizar los datos**

El Agente de Windows Update del dispositivo administrado se conectará al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como orígenes de actualizaciones de Microsoft:

- El Servidor de administración de Kaspersky Security Center Cloud Console (vea los ajustes de la directiva del Agente de red)
- Un servidor Windows Server con Microsoft Windows Server Update Services (WSUS) que se encuentre instalado en la red de su organización
- Los servidores de actualizaciones de Microsoft

Cuando esta opción está habilitada, el Agente de Windows Update del dispositivo administrado se conecta al origen de actualizaciones de Microsoft para obtener información actualizada sobre las actualizaciones de Microsoft Windows aplicables.

Cuando esta opción está deshabilitada, el Agente de actualización de Windows del dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que el origen de actualizaciones brindó en un momento anterior.

Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Podría deshabilitar esta opción si ha configurado un esquema de conexión periódica a este origen en otra tarea o en la sección **Actualizaciones y vulnerabilidades de software** de las propiedades de la directiva del Agente de red. Si no quiere deshabilitar esta opción, para intentar que el Servidor de administración no se sobrecargue, modifique la programación de la tarea para que se la inicie en un punto aleatorio de un intervalo de 360 minutos.

Esta opción está activada de forma predeterminada.

El modo de obtener las actualizaciones deriva de combinar las siguientes opciones de configuración de la directiva del Agente de red:

- El Agente de Windows Update en un dispositivo administrado se conecta al Servidor de actualizaciones para obtener actualizaciones solo si la opción **Conectarse al servidor de actualizaciones para actualizar los datos** está activada en las propiedades de la tarea *Buscar vulnerabilidades y actualizaciones requeridas* y la opción de **Modo de búsqueda de Windows Update** está configurada como **Activo** en la configuración de la directiva del Agente de red.
- Si no necesita el Agente de red para iniciar una conexión al origen de actualizaciones de Microsoft Windows ni para descargar actualizaciones al realizar la tarea *Análisis de vulnerabilidades*, puede seleccionar la opción **Pasivo** en **Modo de búsqueda de Windows Update**, pero la opción **Conectarse al servidor de actualizaciones para actualizar los datos** debe permanecer habilitada. Así podrá ahorrar recursos y usar las actualizaciones de Windows antes recibidas para analizar las vulnerabilidades. Puede usar el modo pasivo si configura la recepción de actualizaciones de Microsoft Windows de otra manera. Si la recepción de actualizaciones de Microsoft Windows no está configurada de otra manera, no seleccione la opción **Pasivo** en **Modo de búsqueda de Windows Update** porque, en este caso, nunca recibirá información sobre las actualizaciones.
- Independientemente del estado de la opción **Conectarse al servidor de actualizaciones para actualizar los datos** (activada o desactivada), si la opción **Deshabilitado** está marcada en **Modo de búsqueda de Windows Update**, Kaspersky Security Center Cloud Console no solicita ninguna información sobre actualizaciones.

- Buscar vulnerabilidades y actualizaciones catalogadas por Kaspersky para software de terceros

Si esta opción está habilitada, Kaspersky Security Center Cloud Console Cloud Console buscará vulnerabilidades y actualizaciones para las aplicaciones de terceros (aplicaciones creadas por proveedores de software que no sean ni Kaspersky ni Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky determina el alcance de la lista de aplicaciones de terceros compatibles.

Si esta opción está deshabilitada, Kaspersky Security Center Cloud Console no buscará vulnerabilidades ni actualizaciones para aplicaciones de terceros. Puede que quiera deshabilitar esta opción si utiliza tareas diferentes, con configuraciones diferentes, para las actualizaciones de Microsoft Windows y para las actualizaciones de aplicaciones de terceros.

Esta opción está activada de forma predeterminada.

- **Especifique las rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**

  Las carpetas en las que Kaspersky Security Center Cloud Console buscará aplicaciones de terceros que deban actualizarse o que tengan vulnerabilidades para reparar. Puede utilizar variables del sistema.

  Especifique las carpetas en las que se instalan las aplicaciones. De manera predeterminada, la lista está vacía.

- **Habilitar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red guardará datos de seguimiento incluso si la función de seguimiento se ha deshabilitado 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. Puede usar la utilidad de diagnóstico remoto para acceder a estos archivos, descargarlos y eliminarlos.

  Si esta función está deshabilitada, el Agente de red determinará si debe o no guardar información de seguimiento guiándose por 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 forma predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

Recomendaciones para programar la tarea

Al programar la tarea *Buscar vulnerabilidades y actualizaciones requeridas*, asegúrese de que las opciones **Ejecutar tareas no realizadas** y **Utilizar retardo aleatorio automático para el inicio de la tarea** estén habilitadas.

De manera predeterminada, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* está configurada para iniciarse de forma manual. Si, debido a las reglas de la organización, los dispositivos se encontraran apagados en el momento en que debiera ejecutarse la tarea, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecutará una vez que los dispositivos se vuelvan a encender, es decir, en la mañana del día siguiente. Esto puede ser inconveniente porque los análisis de vulnerabilidades pueden hacer que aumente la carga en los subsistemas de disco y CPU. Debe buscar que la programación de la tarea se adecue a las reglas dispuestas por su organización.

Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades

La disponibilidad de la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* depende del modo de Kaspersky Security Center Cloud Console y de la licencia que se está utilizando.

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. Puede usar esta tarea para instalar múltiples actualizaciones y reparar múltiples vulnerabilidades utilizando un conjunto de reglas.

Si desea usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar actualizaciones o reparar vulnerabilidades, realice alguna de las siguientes acciones:

- Ejecute el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.
- Cree una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Agregue una regla de instalación de actualizaciones a una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* existente.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia bajo la cual utiliza Kaspersky Security Center Cloud Console y del modo en el que Kaspersky Security Center Cloud Console está funcionando.

Para crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. Para la aplicación 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:
   - **Comenzar la instalación cuando se esté por reiniciar o apagar el dispositivo**

Si esta opción está habilitada, las actualizaciones se instalarán en el momento en el que los dispositivos se reinicien o se apaguen. De lo contrario, las actualizaciones se instalarán siguiendo la programación que se defina.

Utilice esta opción si la instalación de las actualizaciones podría afectar el rendimiento de los dispositivos.

Esta opción está deshabilitada de forma predeterminada.

- **Instalar los componentes generales obligatorios del sistema**

  Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Una actualización podría requerir, por ejemplo, que esté instalada cierta actualización del sistema operativo.

  Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

  Esta opción está deshabilitada de forma predeterminada.

- **Permitir que se instalen versiones nuevas de las aplicaciones durante la actualización**

  Si esta opción está habilitada, las actualizaciones podrán cambiar la versión del software actualizado por una más reciente.

  Si esta opción está deshabilitada, los cambios de versión no estarán permitidos. Para instalar una versión más reciente de una aplicación, deberá usar una tarea diferente o proceder en forma manual. Podría usar esta opción si, por ejemplo, desea evaluar el cambio de versión en una infraestructura de prueba o si sabe que la versión más reciente no es compatible con la infraestructura de su empresa.

  Esta opción está activada de forma predeterminada.

  Los cambios de versión pueden ocasionar problemas de funcionamiento en las aplicaciones dependientes instaladas en los dispositivos cliente.

- **Descargar las actualizaciones en el dispositivo sin instalarlas**

  Si esta opción está habilitada, la aplicación descargará las actualizaciones disponibles en los dispositivos, pero no las instalará automáticamente. Podrá instalar las actualizaciones descargadas manualmente.

  Las actualizaciones de Microsoft se descargan en el sistema de almacenamiento de Windows. Las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft) se descargan en la carpeta especificada en el campo **Descargar actualizaciones en**.

  Si esta opción está deshabilitada, las actualizaciones se instalarán en los dispositivos automáticamente.

  Esta opción está deshabilitada de forma predeterminada.

- **Descargar actualizaciones en**

  Esta carpeta se utiliza para descargar las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft).

- **Habilitar diagnóstico avanzado**

Si esta función está habilitada, el Agente de red guardará datos de seguimiento incluso si la función de seguimiento se ha deshabilitado 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. Puede usar la utilidad de diagnóstico remoto para acceder a estos archivos, descargarlos y eliminarlos.

Si esta función está deshabilitada, el Agente de red determinará si debe o no guardar información de seguimiento guiándose por 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 forma predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

7. Defina las opciones de reinicio del sistema operativo:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

Si no habilita esta opción, la solicitud se mostrará una sola vez.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Tiempo de espera antes del cierre forzado de aplicaciones en sesiones bloqueadas (min)**

  Las aplicaciones se cerrarán por la fuerza cuando el dispositivo del usuario se bloquee (sea manualmente o en forma automática tras un tiempo de inactividad).

  Si esta opción está habilitada, las aplicaciones del dispositivo bloqueado se cerrarán por la fuerza luego de transcurra el intervalo especificado en el campo de entrada.

  Si esta opción está deshabilitada, las aplicaciones del dispositivo bloqueado no se cerrarán.

  Esta opción está deshabilitada de forma predeterminada.

8. Si habilita la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**, 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 de la licencia que se está utilizando.

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 agregar una regla al crear una nueva tarea Instalar actualizaciones requeridas y reparar vulnerabilidades.
- Agregue la regla en la pestaña **Configuración de la aplicación** de la ventana de propiedades de una tarea de *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Utilice el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.

Para agregar una nueva regla para todas las actualizaciones, haga lo siguiente:

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para todas las actualizaciones**.

3. En la página **Criterios generales**, use las listas desplegables para definir los siguientes ajustes:

   - **Conjunto de actualizaciones para instalar**

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - **Reparar vulnerabilidades que tengan o superen este nivel de gravedad**

Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

Esta opción está deshabilitada de forma predeterminada.

4. En la página **Actualizaciones**, seleccione las actualizaciones que se instalarán:

- Instalar todas las actualizaciones adecuadas

  Se instalarán todas las actualizaciones de software que cumplan con los criterios especificados en la página **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

- Instalar solo las actualizaciones de la lista

  Se instalarán únicamente las actualizaciones de software que seleccione manualmente en la lista. La lista contiene todas las actualizaciones de software disponibles.

  Existen situaciones en las que querrá elegir manualmente las actualizaciones que se instalarán: podría suceder, por ejemplo, que quiera evaluar ciertas actualizaciones en un entorno de prueba, que quiera actualizar solo las aplicaciones que considere importantes o que necesite actualizar solo algunas aplicaciones puntuales.

- Instalar automáticamente todas las actualizaciones de aplicaciones previas requeridas para instalar las actualizaciones seleccionadas

  Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

  Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

  A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

  Esta opción está activada de forma predeterminada.

5. En la página **Vulnerabilidades**, seleccione las vulnerabilidades que se repararán al instalar las actualizaciones seleccionadas:

- Reparar todas las vulnerabilidades que coincidan con otros criterios

  Se repararán todas las vulnerabilidades que cumplan con los criterios especificados en la página **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

- Reparar solo las vulnerabilidades de la lista

  Se repararán únicamente las vulnerabilidades que seleccione manualmente en la lista. La lista contiene todas las vulnerabilidades detectadas.

  Existen situaciones en las que querrá elegir manualmente las vulnerabilidades que se repararán: podría suceder, por ejemplo, que quiera verificar en un entorno de prueba que las vulnerabilidades se puedan reparar, que quiera reparar las vulnerabilidades solo en las aplicaciones que considere importantes o que prefiera reparar las vulnerabilidades solo en ciertas aplicaciones puntuales.

6. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas llegue a su fin, se agregará la nueva regla. La encontrará en la lista de reglas del Asistente para crear nueva tarea o en las propiedades de la tarea.

Para agregar una nueva regla para actualizaciones de Windows Update, haga lo siguiente:

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para Windows Update**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - Reparar vulnerabilidades que tengan o superen este nivel de gravedad

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

     Esta opción está deshabilitada de forma predeterminada.

   - Reparar vulnerabilidades con un nivel de gravedad de MSRC igual o mayor que

Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

Esta opción está deshabilitada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Categorías de actualizaciones**, seleccione las categorías de actualizaciones que se instalarán. Las categorías son las mismas que se usan en el Catálogo de Microsoft Update. Por defecto, están seleccionadas todas las categorías.

6. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas llegue a su fin, se agregará la nueva regla. La encontrará en la lista de reglas del Asistente para crear nueva tarea o en las propiedades de la tarea.

Para agregar una nueva regla para actualizaciones de aplicaciones de terceros, haga lo siguiente:

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para las actualizaciones de terceros**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - Reparar vulnerabilidades que tengan o superen este nivel de gravedad

Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

Esta opción está deshabilitada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección Configuración de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas llegue a su fin, se agregará la nueva regla. La encontrará en la lista de reglas del Asistente para crear nueva tarea o en las propiedades de la tarea.

Crear la tarea Instalar actualizaciones de Windows Update

La tarea "Instalar actualizaciones de Windows Update" permite instalar en los dispositivos cliente las actualizaciones de software que proporciona el servicio de Windows Update.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia bajo la cual utiliza Kaspersky Security Center Cloud Console y del modo en el que Kaspersky Security Center Cloud Console está funcionando.

Para crear la tarea "Instalar actualizaciones de Windows Update":

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

2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. Para la aplicación 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 **Agregar**.

   Se abre la lista de actualizaciones.

7. Seleccione las actualizaciones de Windows Update que desee instalar y, a continuación, haga clic en **Aceptar**.

8. Defina las opciones de reinicio del sistema operativo:

- **No reiniciar el dispositivo**

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- **Reiniciar el dispositivo**

  Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

  Si no habilita esta opción, la solicitud se mostrará una sola vez.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

Esta opción está deshabilitada de forma predeterminada.

9. Configure los ajustes relativos a la cuenta:

- **Cuenta predeterminada**

  La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

  Esta opción está seleccionada de forma predeterminada.

- **Especificar cuenta**

  Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

- **Cuenta**

  Cuenta con la que se ejecutará la tarea.

- **Contraseña**

  Contraseña de la cuenta con la que se ejecutará la tarea.

10. Si desea modificar la configuración predeterminada de la tarea, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**. Si no habilita esta opción, la tarea se creará con la configuración predeterminada. Podrá modificar la configuración predeterminada en cualquier otro momento.

11. Haga clic en el botón **Finalizar**.

    Se crea la tarea y se la agrega a la lista de tareas.

12. Haga clic en el nombre de la nueva tarea para abrir la ventana de propiedades de la tarea.

13. En la ventana de propiedades de la tarea, modifique los ajustes generales de la tarea según resulte necesario.

14. Haga clic en el botón **Guardar**.

La tarea queda creada y configurada.

Ver información sobre las actualizaciones disponibles para el software de terceros

Puede ver la lista de actualizaciones disponibles para las aplicaciones de terceros instaladas en los dispositivos cliente (incluidas las aplicaciones de Microsoft).

Para ver una lista de las actualizaciones disponibles para las aplicaciones de terceros instaladas en los dispositivos cliente,

En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Actualizaciones de software**.

Se mostrará una lista con las actualizaciones disponibles.

Puede aplicar un filtro para ver la lista de actualizaciones de software. Para definir el filtro, haga clic en el ícono **Filtrar** ( ) ubicado en la esquina superior derecha de la lista de actualizaciones de software. También puede elegir un filtro preestablecido de la lista desplegable **Filtros preestablecidos**, que se encuentra sobre la lista de vulnerabilidades de software.

Para ver las propiedades de una actualización:

1. Haga clic en el nombre de la actualización de software que sea de su interés.
2. Se abre la ventana de propiedades de la actualización, que consta de las siguientes pestañas con información:

- **General**

  Esta pestaña contiene los detalles generales de la actualización seleccionada:

  - Estado de aprobación de la actualización (si desea cambiar este estado, puede elegir uno diferente en la lista desplegable)
  - Categoría de Windows Server Update Services (WSUS) a la que pertenece la actualización
  - Fecha y hora en que se registró la actualización
  - Fecha y hora en que se creó la actualización
  - Nivel de importancia de la actualización
  - Requisitos de instalación impuestos por la actualización
  - Familia de aplicaciones a la que pertenece la actualización
  - Aplicación a la que corresponde la actualización
  - Número de revisión de la actualización

- **Atributos**

Esta pestaña muestra una serie de atributos que permiten buscar más información sobre la actualización seleccionada. Los atributos disponibles dependen de si la actualización fue publicada por Microsoft o por otro desarrollador.

Cuando una actualización proviene de Microsoft, la información disponible en la pestaña es la siguiente:

- Nivel de importancia asignado a la actualización por el Centro de respuestas de seguridad de Microsoft (MSRC)
- Vínculo al artículo de Microsoft Knowledge Base en el que se describe la actualización
- Vínculo al artículo del boletín de seguridad de Microsoft en el que se describe la actualización
- Identificador (id.) de la actualización

Cuando una actualización proviene de otro desarrollador, la información disponible en la pestaña es la siguiente:

- Indicador de si la actualización es un parche o un paquete de distribución completo
- Idioma de localización de la actualización
- Indicador de si la actualización se instaló de forma manual o automática
- Indicador de si la actualización se revocó tras ser instalada
- Vínculo de descarga de la actualización

- **Dispositivos**

  Esta pestaña contiene la lista de dispositivos en los que se encuentra instalada la actualización elegida.

- **Vulnerabilidades reparadas**

  Esta pestaña contiene la lista de vulnerabilidades que pueden repararse con la actualización seleccionada.

- **Cruce de actualizaciones**

  Esta pestaña muestra cualquier "cruce" que pueda existir entre las actualizaciones publicadas para una misma aplicación; en otras palabras, aquí se indica si la actualización seleccionada puede reemplazar a otras actualizaciones o si, por el contrario, puede ser reemplazada por otras. Esta información solo está disponible para actualizaciones de Microsoft.

- **Tareas para instalar esta actualización**

  Esta pestaña contiene una lista de tareas que, por su alcance, pueden usarse para instalar la actualización seleccionada. Desde aquí también se puede crear una nueva tarea de instalación remota para la actualización.

Para ver las estadísticas de instalación de una actualización:

1. Marque la casilla ubicada junto a la actualización de software que sea de su interés.

2. Haga clic en el botón **Estadísticas de los estados de instalación de la actualización**.

   Se muestra un diagrama con los estados de instalación de la actualización. Si hace clic en un estado, se abrirá una lista con los dispositivos en los que la actualización tenga el estado seleccionado.

Puede ver información sobre las actualizaciones de software disponibles para el software de terceros (incluido el software de Microsoft) instalado en un dispositivo con Windows en particular.

Para ver una lista de las actualizaciones disponibles para el software de terceros instalado en un dispositivo administrado específico:

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

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo sobre el que quiera información.

   Se muestra la ventana de propiedades del dispositivo seleccionado.

3. En la ventana de propiedades del dispositivo seleccionado, elija la pestaña **Avanzado**.

4. En el panel de la izquierda, elija la sección **Actualizaciones disponibles**. Si solo desea ver las actualizaciones instaladas, seleccione la opción **Mostrar actualizaciones instaladas**.

   Se muestra la lista de actualizaciones de software de terceros disponibles para el dispositivo seleccionado.

Exportar la lista de actualizaciones de software disponibles a un archivo

Puede exportar a un archivo CSV o TXT la lista de actualizaciones disponibles para las aplicaciones de terceros (incluidas las de Microsoft) que se muestra en un momento dado. Una vez que tenga el archivo, podrá almacenarlo para fines estadísticos, enviarlo a la persona que esté a cargo de la seguridad de la información o utilizarlo para otros fines.

Para exportar a un archivo de texto la lista de actualizaciones disponibles para el software de terceros instalado en todos los dispositivos administrados:

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Actualizaciones de software**.

   La página muestra una lista de actualizaciones disponibles para el software de terceros instalado en todos los dispositivos administrados.

2. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera.

   El archivo con la lista de actualizaciones disponibles para el software de terceros, incluido el software de Microsoft, se guardará en el dispositivo que esté utilizando.

Para exportar a un archivo de texto la lista de actualizaciones disponibles para el software de terceros instalado en un dispositivo administrado específico:

1. Abra la lista de actualizaciones de software de terceros disponibles para el dispositivo administrado pertinente.

2. Seleccione las actualizaciones de software que desee exportar.

   Omita este paso si desea exportar toda la lista de actualizaciones de software.

   Si desea exportar la lista completa de actualizaciones de software, tenga en cuenta que solo se exportarán las actualizaciones que aparezcan en la página que esté viendo.

   Si desea exportar solo las actualizaciones instaladas, marque la casilla **Mostrar actualizaciones instaladas**.

3. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera.

En el dispositivo que esté utilizando, se guardará un archivo con la lista de actualizaciones disponibles para el software de terceros (incluido el software de Microsoft) instalado en el dispositivo administrado seleccionado.

Aprobar y rechazar actualizaciones de software de terceros

Al configurar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede crear una regla que exija que las actualizaciones que se deban instalar tengan un estado específico. Una regla de actualización puede permitir, por ejemplo, la instalación de estas actualizaciones:

- Solo las actualizaciones aprobadas
- Solo las actualizaciones aprobadas o sin estado definido
- Todas las actualizaciones, independientemente de su estado

Puede aprobar las actualizaciones que deban instalarse y rechazar las que no deban instalarse.

Puede usar el estado *Aprobada* para administrar la instalación de un número modesto de actualizaciones. Cuando necesite instalar muchas actualizaciones, utilice en cambio las reglas que puede configurar en la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Asigne el estado *Aprobada* únicamente a las actualizaciones que no cumplan con los criterios indicados en las reglas. Aprobar un gran número de actualizaciones en forma manual afecta el rendimiento del Servidor de administración y puede, incluso, hacer que se sobrecargue.

Para aprobar o rechazar una o más actualizaciones:

1. En el menú principal, vaya a **Operaciones → Administración de parches → Actualizaciones de software**.

   Se mostrará una lista con las actualizaciones disponibles.

2. Seleccione las actualizaciones que desee aprobar o rechazar.

3. Haga clic en **Aprobar** para aprobar las actualizaciones seleccionadas o en **Rechazar** para rechazarlas.

   El valor predeterminado es *Sin definir*.

Los estados de las actualizaciones seleccionadas cambian a los que ha elegido.

Como alternativa, puede cambiar el estado de aprobación en las propiedades de una actualización específica.

Para aprobar o rechazar una actualización desde sus propiedades:

1. En el menú principal, vaya a **Operaciones → Administración de parches → Actualizaciones de software**.

   Se mostrará una lista con las actualizaciones disponibles.

2. Haga clic en el nombre de la actualización que desee aprobar o rechazar.

   Se abre la ventana de propiedades de la actualización.

3. En la sección **General**, cambie la opción **Estado de aprobación de la actualización** para elegir el estado de la actualización. Puede seleccionar los estados *Aprobada*, *Rechazada* o *Sin definir*.

4. Haga clic en el botón **Guardar** para guardar los cambios.

El estado de la actualización seleccionada cambia al que ha elegido.

Si asigna el estado **Rechazada** a las actualizaciones de software de un tercero, estas no se instalarán en los dispositivos a los que estén asignadas, pero que aún no las hayan recibido. Las actualizaciones no se eliminarán de los dispositivos en los que ya se encuentren instaladas. Si necesita eliminar estas actualizaciones, hágalo manualmente en forma local.

Actualización automática de aplicaciones de terceros

Algunas aplicaciones de terceros se pueden actualizar automáticamente. Quien determina si una aplicación es compatible con la función de actualización automática es su desarrollador o proveedor. Si una aplicación de terceros instalada en un dispositivo administrado se puede actualizar automáticamente, podrá configurar el ajuste de actualización automática en las propiedades de esa aplicación. Luego de que modifique este ajuste, las instancias del Agente de red implementarán el nuevo valor en cada dispositivo administrado que tenga instalada esa aplicación.

El ajuste de actualización automática es independiente de los demás objetos y ajustes de la característica Administración de vulnerabilidades y parches. Este ajuste, por ejemplo, no se ve afectado por los estados de aprobación de las actualizaciones ni por las distintas tareas de instalación de actualizaciones, como *Instalar actualizaciones requeridas y reparar vulnerabilidades*, *Instalar actualizaciones de Windows Update* y *Reparar vulnerabilidades*.

Para configurar el ajuste de actualización automática para una aplicación creada por un tercero:

1. En el menú principal, vaya a **Operaciones → Aplicaciones de terceros → Registro de aplicaciones**.

2. Haga clic en el nombre de la aplicación para la que desee modificar el ajuste de actualización automática.

   Puede usar la columna **Estado de las actualizaciones automáticas** para filtrar la lista y simplificar la búsqueda.

   Se abrirá la ventana de propiedades de la aplicación.

3. En la sección **General**, seleccione un valor para el siguiente ajuste:

   Estado de las actualizaciones automáticas

Seleccione una de las siguientes opciones:

- **Sin definir**

  Se deshabilitará la función de actualización automática. Kaspersky Security Center Cloud Console instalará las actualizaciones de la aplicación a través de las 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 instalará las actualizaciones de la aplicación a través de las 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 reparar vulnerabilidades de software

Kaspersky Security Center Cloud Console detecta y repara vulnerabilidades de software en dispositivos administrados que ejecutan los sistemas operativos de Microsoft Windows. La solución puede detectar vulnerabilidades tanto en el sistema operativo como en aplicaciones desarrolladas por Microsoft y otros terceros.

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

Búsqueda de vulnerabilidades de software

Para encontrar vulnerabilidades de software, Kaspersky Security Center Cloud Console utiliza características de dos recursos: la base de datos de Windows Update y la base de datos de vulnerabilidades conocidas. Este último es un recurso creado y mantenido por 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.

Para encontrar vulnerabilidades de software, Kaspersky Security Center Cloud Console utiliza la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

Reparación de vulnerabilidades de software

Para reparar vulnerabilidades de software, Kaspersky Security Center Cloud Console utiliza las actualizaciones de software que publican los proveedores de software. La lista de vulnerabilidades de software está a disposición para que la vea en cualquier momento. Los metadatos de las actualizaciones de software se descargan en el repositorio del Servidor de administración de manera automática, y se copian a los repositorios de los puntos de distribución cuando se ejecuta la tarea *Descargar actualizaciones en los repositorios de los puntos de distribución*. Puede crear esta tarea manualmente o a través del asistente de inicio rápido de Kaspersky Security Center Cloud Console.

Las actualizaciones de software con las que se corrigen las vulnerabilidades pueden ser paquetes de distribución completos o parches. Las actualizaciones de software diseñadas para corregir vulnerabilidades de software se denominan *reparaciones*. En Kaspersky Security Center Cloud Console, las vulnerabilidades se corrigen utilizando *reparaciones recomendadas*. Las reparaciones recomendadas son las actualizaciones de software que los especialistas de Kaspersky recomiendan instalar.

Dependiendo del modo de Kaspersky Security Center Cloud Console y de la licencia que esté utilizando, podrá usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Reparar vulnerabilidades* para reparar vulnerabilidades de software.

La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* puede corregir varias vulnerabilidades a la vez. A tal fin, instala automáticamente las reparaciones que se recomiendan para el caso. Si utiliza esta tarea, puede configurar manualmente ciertas reglas para la reparación de distintas vulnerabilidades.

La tarea *Reparar vulnerabilidades*, por su parte, puede usarse para instalar las reparaciones recomendadas para las vulnerabilidades en el software de Microsoft.

Por seguridad, cada actualización de software de terceros que se instala con la función Administración de vulnerabilidades y parches se somete a un análisis antimalware automático con las tecnologías de Kaspersky Estas tecnologías revisan automáticamente los archivos utilizando técnicas de análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno de pruebas y aprendizaje automático, entre otras.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. Tampoco buscan vulnerabilidades (conocidas o desconocidas) o funciones no documentadas en las actualizaciones ni las analizan de modos que no se hayan indicado en el párrafo anterior.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia bajo la cual utiliza Kaspersky Security Center Cloud Console y del modo en el que Kaspersky Security Center Cloud Console está funcionando.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

Para reparar algunas vulnerabilidades de software, deberá aceptar un contrato de licencia de usuario final (EULA) que lo faculte a instalar el software. Si se le solicita aceptar el EULA, hágalo. Rechazar el EULA impedirá reparar la vulnerabilidad en cuestión.

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 bajo la cual utiliza Kaspersky Security Center Cloud Console y del modo en el que Kaspersky Security Center Cloud Console está funcionando.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación afectada está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

Como alternativa, para crear una tarea para reparar vulnerabilidades de software, puede optar por estas vías:

- Abra la lista de vulnerabilidades y seleccione las vulnerabilidades que desee reparar.

  Como resultado, se creará una nueva tarea para reparar las vulnerabilidades de software seleccionadas. Si lo prefiere, puede agregar las vulnerabilidades seleccionadas a una tarea existente.

- Utilice el Asistente de reparación de vulnerabilidades.

  La disponibilidad de esta función depende del modo de Kaspersky Security Center Cloud Console y de la licencia que se está utilizando.

  El asistente simplifica la creación y configuración de tareas de reparación de vulnerabilidades. También evita que se creen tareas redundantes, que tengan las mismas actualizaciones para instalar.

Reparar vulnerabilidades de software a través de la lista de vulnerabilidades

Para reparar vulnerabilidades de software:

1. Abra una de las listas de vulnerabilidades:

   - Para abrir la lista de vulnerabilidades general, en el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.

   - Para abrir la lista de vulnerabilidades de un dispositivo administrado, en el menú principal, vaya a **Activos (dispositivos)** → **Dispositivos administrados** → **<nombre del dispositivo>** → **Avanzado** → **Vulnerabilidades de software**.

   - Para abrir la lista de vulnerabilidades de una aplicación específica, en el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Registro de aplicaciones** → **<nombre de la aplicación>** → **Vulnerabilidades**.

   Se muestra una página con una lista de vulnerabilidades detectadas en las aplicaciones de terceros.

2. Seleccione una o más vulnerabilidades de la lista y haga clic en el botón **Reparar vulnerabilidad**.

   Si no se cuenta con la actualización de software recomendada para reparar alguna de las vulnerabilidades seleccionadas, se mostrará un mensaje informativo.

   Para reparar algunas vulnerabilidades de software, 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, no se reparará la vulnerabilidad de software correspondiente.

3. Seleccione una de las siguientes opciones:

- **Nueva tarea**

  Se inicia el Asistente para crear nueva tarea. Dependiendo del modo de Kaspersky Security Center Cloud Console y de la licencia que esté utilizando, estará 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 (agregar regla a la tarea especificada)**

  Seleccione la tarea a la que desee agregar las vulnerabilidades seleccionadas. Dependiendo del modo de Kaspersky Security Center Cloud Console y de la licencia que esté utilizando, seleccione una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o una tarea *Reparar vulnerabilidades*. Si selecciona una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, se agregará automáticamente una nueva regla a esa tarea para corregir las vulnerabilidades seleccionadas. Si selecciona una tarea *Reparar vulnerabilidades*, las vulnerabilidades seleccionadas se agregarán a las propiedades de la tarea.

  Se abrirá la ventana de propiedades de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

Si optó por crear una tarea, se la creará y se la agregará a la lista de tareas disponible en **Activos (dispositivos)** → **Tareas**. Si optó por agregar las vulnerabilidades a una tarea existente, las vulnerabilidades se guardarán en las propiedades de la tarea que haya elegido.

Para reparar las vulnerabilidades de software de terceros, inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Reparar vulnerabilidades*. Si la tarea que creó es *Reparar vulnerabilidades*, deberá especificar manualmente qué actualizaciones se usarán para reparar las vulnerabilidades enumeradas en la configuración de la tarea.

Reparar vulnerabilidades de software con el Asistente de reparación de vulnerabilidades

La disponibilidad del Asistente de reparación de vulnerabilidades depende de la licencia que se está utilizando y del modo de funcionamiento de Kaspersky Security Center Cloud Console.

Para reparar vulnerabilidades de software a través del Asistente de reparación de vulnerabilidades:

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.

   Se muestra una página con una lista de las vulnerabilidades detectadas en las aplicaciones de terceros instaladas en los dispositivos administrados.

2. Marque la casilla ubicada junto a la vulnerabilidad que desee reparar.

3. Haga clic en el botón **Ejecutar el Asistente de reparación de vulnerabilidades**.

   Se iniciará el Asistente de reparación de vulnerabilidades. En la página **Seleccione una tarea de reparación de vulnerabilidades**, verá una lista con las tareas existentes de los siguientes tipos:

   - *Instalar actualizaciones requeridas y reparar vulnerabilidades*
   - *Instalar actualizaciones de Windows Update*
   - *Reparar vulnerabilidades*

   Los dos últimos tipos de tarea no se pueden modificar para instalar nuevas actualizaciones. Para instalar nuevas actualizaciones, solo puede utilizar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

4. Si desea que el asistente muestre solo las tareas que permitan reparar la vulnerabilidad seleccionada, habilite la opción **Mostrar solo las tareas que permitan reparar esta vulnerabilidad**.

5. Elija lo que desea hacer:

   - Para iniciar una tarea, marque la casilla ubicada junto al nombre de la tarea en cuestión y haga clic en el botón **Iniciar**.

   - Para agregar una nueva regla a una tarea existente, haga lo siguiente:

     a. Marque la casilla ubicada junto al nombre de la tarea pertinente y haga clic en el botón **Agregar regla**.

     b. En la página que se abrirá, configure la nueva regla:

     - Regla para reparar vulnerabilidades de este nivel de gravedad

       Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

       Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

       Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

       Esta opción está deshabilitada de forma predeterminada.

     - **Regla para reparar vulnerabilidades por medio de actualizaciones del mismo tipo que la actualización definida como recomendada para la vulnerabilidad seleccionada** (disponible solo para vulnerabilidades de software de Microsoft)

     - **Regla para reparar vulnerabilidades en las aplicaciones del proveedor seleccionado** (disponible solo para vulnerabilidades de software de terceros)

     - **Regla para reparar una vulnerabilidad en todas las versiones de la aplicación seleccionada** (disponible solo para vulnerabilidades de software de terceros)

     - **Regla para reparar la vulnerabilidad seleccionada**

     - Aprobar actualizaciones que reparen esta vulnerabilidad

       Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

       Esta opción está deshabilitada de forma predeterminada.

     c. Haga clic en el botón **Agregar**.

   - Para crear una tarea:

     a. Haga clic en el botón **Nueva tarea**.

     b. En la página que se abrirá, configure la nueva regla:

- Regla para reparar vulnerabilidades de este nivel de gravedad

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al nivel de gravedad de la actualización seleccionada. Los niveles posibles son **Medio**, **Alto** y **Crítico**. Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

  Esta opción está deshabilitada de forma predeterminada.

- **Regla para solucionar vulnerabilidades mediante el uso de actualizaciones del tipo** (disponible solo para vulnerabilidades de software de Microsoft)
- **Regla para reparar vulnerabilidades en las aplicaciones del proveedor seleccionado** (disponible solo para vulnerabilidades de software de terceros)
- **Regla para reparar una vulnerabilidad en todas las versiones de la aplicación seleccionada** (disponible solo para vulnerabilidades de software de terceros)
- **Regla para reparar la vulnerabilidad seleccionada**
- Aprobar actualizaciones que reparen esta vulnerabilidad

  Se aprobará la instalación de la actualización seleccionada. Habilite esta opción si ha aplicado reglas de instalación de actualizaciones que solo permitan instalar actualizaciones aprobadas.

  Esta opción está deshabilitada de forma predeterminada.

c. Haga clic en el botón **Agregar**.

Si eligió iniciar una tarea, puede cerrar el asistente. La tarea se completará en segundo plano. No se requieren más acciones.

Si optó por agregar una regla a una tarea existente, se abrirá la ventana de propiedades de la tarea. Encontrará la nueva regla en las propiedades de la tarea. Si lo desea, vea y modifique la regla u otros ajustes de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

Si eligió crear una tarea, continúe creándola en el Asistente para crear nueva tarea. La nueva regla que haya agregado en el Asistente de reparación de vulnerabilidades aparecerá en el Asistente para crear nueva tarea. Una vez que complete los pasos del Asistente para crear nueva tarea, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se agregará a la lista de tareas.

Crear la tarea Reparar vulnerabilidades

La tarea *Reparar vulnerabilidades* permite reparar vulnerabilidades en las aplicaciones Microsoft de los dispositivos administrados que ejecutan Windows.

La disponibilidad de esta función depende del modo de Kaspersky Security Center Cloud Console y de la licencia que se está utilizando. Le recomendamos que utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* en lugar de la tarea *Reparar vulnerabilidades*. La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* le permitirá instalar múltiples actualizaciones y reparar múltiples vulnerabilidades simultánea y automáticamente utilizando un conjunto de reglas.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia bajo la cual utiliza Kaspersky Security Center Cloud Console y del modo en el que Kaspersky Security Center Cloud Console está funcionando.

Para actualizar una aplicación de terceros o reparar una vulnerabilidad en una aplicación de terceros instalada en un dispositivo administrado, podría necesitarse la colaboración del usuario. Si la aplicación está abierta, por ejemplo, podría tener que pedirle al usuario que la cierre.

Para crear la tarea Reparar vulnerabilidades:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. 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 **Agregar**.

   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 mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

   - **Reiniciar el dispositivo**

     Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

   - **Solicitar al usuario una acción**

A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

  Si no habilita esta opción, la solicitud se mostrará una sola vez.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de aplicaciones en sesiones bloqueadas**

  Las aplicaciones abiertas en el dispositivo cliente podrían impedir que se lo reinicie. Si el usuario está editando un documento en un procesador de textos, por ejemplo, y no ha guardado el archivo, el procesador de textos no permitirá que el dispositivo se reinicie.

  Si habilita esta opción, las aplicaciones que se estén ejecutando en un dispositivo bloqueado se cerrarán por la fuerza y, tras ello, el dispositivo se reiniciará. Los usuarios podrían perder los cambios que no hayan guardado.

  Si no habilita esta opción, los dispositivos bloqueados no se reiniciarán. El estado de la tarea en tales dispositivos indicará que hay un reinicio pendiente. Los usuarios tendrán que cerrar manualmente todas las aplicaciones abiertas para luego reiniciar sus dispositivos.

  Esta opción está deshabilitada de forma predeterminada.

9. Configure los ajustes relativos a la cuenta:

- **Cuenta predeterminada**

  La tarea se ejecutará utilizando la misma cuenta que la aplicación que realizará la tarea.

  Esta opción está seleccionada de forma predeterminada.

- **Especificar cuenta**

  Complete los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta con la que se ejecutará la tarea. La cuenta debe tener los derechos necesarios para realizar la tarea.

- **Cuenta**

  Cuenta con la que se ejecutará la tarea.

- **Contraseña**

  Contraseña de la cuenta con la que se ejecutará la tarea.

10. Si habilita la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**, 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 Kaspersky Security Center Cloud Console y de la licencia que se está utilizando.

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. Puede usar esta tarea para instalar múltiples actualizaciones y reparar múltiples vulnerabilidades utilizando un conjunto de reglas.

Si desea usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* para instalar actualizaciones o reparar vulnerabilidades, realice alguna de las siguientes acciones:

- Ejecute el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.
- Cree una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Agregue una regla de instalación de actualizaciones a una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* existente.

Las tareas de instalación de actualizaciones de software tienen una serie de limitaciones. Estas limitaciones dependen de la licencia bajo la cual utiliza Kaspersky Security Center Cloud Console y del modo en el que Kaspersky Security Center Cloud Console está funcionando.

Para crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades:

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

2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.

3. Para la aplicación 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:

   - **Comenzar la instalación cuando se esté por reiniciar o apagar el dispositivo**

     Si esta opción está habilitada, las actualizaciones se instalarán en el momento en el que los dispositivos se reinicien o se apaguen. De lo contrario, las actualizaciones se instalarán siguiendo la programación que se defina.

     Utilice esta opción si la instalación de las actualizaciones podría afectar el rendimiento de los dispositivos.

     Esta opción está deshabilitada de forma predeterminada.

   - **Instalar los componentes generales obligatorios del sistema**

     Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Una actualización podría requerir, por ejemplo, que esté instalada cierta actualización del sistema operativo.

     Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

     Esta opción está deshabilitada de forma predeterminada.

   - **Permitir que se instalen versiones nuevas de las aplicaciones durante la actualización**

     Si esta opción está habilitada, las actualizaciones podrán cambiar la versión del software actualizado por una más reciente.

     Si esta opción está deshabilitada, los cambios de versión no estarán permitidos. Para instalar una versión más reciente de una aplicación, deberá usar una tarea diferente o proceder en forma manual. Podría usar esta opción si, por ejemplo, desea evaluar el cambio de versión en una infraestructura de prueba o si sabe que la versión más reciente no es compatible con la infraestructura de su empresa.

     Esta opción está activada de forma predeterminada.

     Los cambios de versión pueden ocasionar problemas de funcionamiento en las aplicaciones dependientes instaladas en los dispositivos cliente.

   - **Descargar las actualizaciones en el dispositivo sin instalarlas**

Si esta opción está habilitada, la aplicación descargará las actualizaciones disponibles en los dispositivos, pero no las instalará automáticamente. Podrá instalar las actualizaciones descargadas manualmente.

Las actualizaciones de Microsoft se descargan en el sistema de almacenamiento de Windows. Las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft) se descargan en la carpeta especificada en el campo **Descargar actualizaciones en**.

Si esta opción está deshabilitada, las actualizaciones se instalarán en los dispositivos automáticamente.

Esta opción está deshabilitada de forma predeterminada.

- Descargar actualizaciones en

  Esta carpeta se utiliza para descargar las actualizaciones para aplicaciones de terceros (aplicaciones creadas por proveedores de software que no son ni Kaspersky ni Microsoft).

- Habilitar diagnóstico avanzado

  Si esta función está habilitada, el Agente de red guardará datos de seguimiento incluso si la función de seguimiento se ha deshabilitado 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. Puede usar la utilidad de diagnóstico remoto para acceder a estos archivos, descargarlos y eliminarlos.

  Si esta función está deshabilitada, el Agente de red determinará si debe o no guardar información de seguimiento guiándose por 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 forma predeterminada.

- Tamaño máximo, en MB, de los archivos de diagnóstico avanzado

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Los especialistas en soporte técnico de Kaspersky podrían pedirle que cambie el valor predeterminado si, para solucionar un problema, les remite archivos de diagnóstico avanzado con información insuficiente.

7. Defina las opciones de reinicio del sistema operativo:

- No reiniciar el dispositivo

  Cuando termine la operación, los dispositivos cliente no se reiniciarán automáticamente. Para que la operación se complete, deberá reiniciar los dispositivos en forma manual o mediante, por ejemplo, una tarea de administración de dispositivos. Los resultados de la tarea y el estado de cada dispositivo darán cuenta de que hay un reinicio pendiente. Esta opción es útil cuando la tarea va a ejecutarse en servidores y dispositivos que deben operar continuamente.

- Reiniciar el dispositivo

Los dispositivos cliente se reiniciarán automáticamente siempre que resulte necesario para completar la operación. Esta opción es útil cuando la tarea se realiza en dispositivos que admiten una breve interrupción para apagarse o reiniciarse.

- **Solicitar al usuario una acción**

  A través de un recordatorio en pantalla, se le pedirá a cada usuario que reinicie su dispositivo manualmente. Puede configurar algunos ajustes avanzados para esta opción: el texto del mensaje que se le muestra al usuario, la frecuencia con la que se muestra este mensaje y el tiempo que se espera antes de reiniciar el dispositivo por la fuerza (sin que el usuario confirme el reinicio). Esta opción es la más adecuada para estaciones de trabajo en las que los usuarios deben poder seleccionar el momento más conveniente para reiniciar.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si habilita esta opción, la aplicación le solicitará al usuario que reinicie su sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo por defecto es de 5 minutos. Los valores disponibles van de 1 a 1440 minutos.

  Si no habilita esta opción, la solicitud se mostrará una sola vez.

- **Reiniciar después de (min)**

  Tras mostrarle una solicitud al usuario y aguardar el tiempo especificado, la aplicación reiniciará el sistema operativo por la fuerza.

  Esta opción está activada de forma predeterminada. El tiempo de espera por defecto es de 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Tiempo de espera antes del cierre forzado de aplicaciones en sesiones bloqueadas (min)**

  Las aplicaciones se cerrarán por la fuerza cuando el dispositivo del usuario se bloquee (sea manualmente o en forma automática tras un tiempo de inactividad).

  Si esta opción está habilitada, las aplicaciones del dispositivo bloqueado se cerrarán por la fuerza luego de transcurra el intervalo especificado en el campo de entrada.

  Si esta opción está deshabilitada, las aplicaciones del dispositivo bloqueado no se cerrarán.

  Esta opción está deshabilitada de forma predeterminada.

8. Si habilita la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de la tarea**, 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 de la licencia que se está utilizando.

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 agregar una regla al crear una nueva tarea Instalar actualizaciones requeridas y reparar vulnerabilidades.
- Agregue la regla en la pestaña **Configuración de la aplicación** de la ventana de propiedades de una tarea de *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Utilice el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.

Para agregar una nueva regla para todas las actualizaciones, haga lo siguiente:

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para todas las actualizaciones**.

3. En la página **Criterios generales**, use las listas desplegables para definir los siguientes ajustes:

   - **Conjunto de actualizaciones para instalar**

Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

- **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
- **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
- **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

- Reparar vulnerabilidades que tengan o superen este nivel de gravedad

Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

Esta opción está deshabilitada de forma predeterminada.

4. En la página **Actualizaciones**, seleccione las actualizaciones que se instalarán:

- Instalar todas las actualizaciones adecuadas

Se instalarán todas las actualizaciones de software que cumplan con los criterios especificados en la página **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

- Instalar solo las actualizaciones de la lista

Se instalarán únicamente las actualizaciones de software que seleccione manualmente en la lista. La lista contiene todas las actualizaciones de software disponibles.

Existen situaciones en las que querrá elegir manualmente las actualizaciones que se instalarán: podría suceder, por ejemplo, que quiera evaluar ciertas actualizaciones en un entorno de prueba, que quiera actualizar solo las aplicaciones que considere importantes o que necesite actualizar solo algunas aplicaciones puntuales.

- Instalar automáticamente todas las actualizaciones de aplicaciones previas requeridas para instalar las actualizaciones seleccionadas

Mantenga habilitada esta opción si está de acuerdo en que, para instalar las actualizaciones seleccionadas, se instalen versiones intermedias de las aplicaciones.

Si deshabilita esta opción, se instalarán únicamente las versiones de las aplicaciones que haya seleccionado. Deshabilite esta opción si quiere que las aplicaciones se actualicen en forma directa, sin que se trate de instalar versiones intermedias. Cuando las actualizaciones seleccionadas no se puedan instalar sin que antes se instalen versiones más antiguas de las aplicaciones, el proceso de actualización no se completará.

A modo de ejemplo, imagine que un dispositivo tiene instalada la versión 3 de una aplicación. Quiere actualizar esa versión a la 5, pero la versión 5 solo se puede instalar sobre la versión 4. Si esta opción está habilitada, el software instalará primero la versión 4 y luego la versión 5. Si esta opción está deshabilitada, el software no podrá actualizar la aplicación.

Esta opción está activada de forma predeterminada.

5. En la página **Vulnerabilidades**, seleccione las vulnerabilidades que se repararán al instalar las actualizaciones seleccionadas:

   - **Reparar todas las vulnerabilidades que coincidan con otros criterios**

     Se repararán todas las vulnerabilidades que cumplan con los criterios especificados en la página **Criterios generales** del asistente. Esta es la opción seleccionada por defecto.

   - **Reparar solo las vulnerabilidades de la lista**

     Se repararán únicamente las vulnerabilidades que seleccione manualmente en la lista. La lista contiene todas las vulnerabilidades detectadas.

     Existen situaciones en las que querrá elegir manualmente las vulnerabilidades que se repararán: podría suceder, por ejemplo, que quiera verificar en un entorno de prueba que las vulnerabilidades se puedan reparar, que quiera reparar las vulnerabilidades solo en las aplicaciones que considere importantes o que prefiera reparar las vulnerabilidades solo en ciertas aplicaciones puntuales.

6. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas llegue a su fin, se agregará la nueva regla. La encontrará en la lista de reglas del Asistente para crear nueva tarea o en las propiedades de la tarea.

Para agregar una nueva regla para actualizaciones de Windows Update, haga lo siguiente:

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para Windows Update**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

   - **Conjunto de actualizaciones para instalar**

Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

- **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
- **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
- **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

- Reparar vulnerabilidades que tengan o superen este nivel de gravedad

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

  Esta opción está deshabilitada de forma predeterminada.

- Reparar vulnerabilidades con un nivel de gravedad de MSRC igual o mayor que

  Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

  Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que el Centro de respuestas de seguridad de Microsoft (MSRC) haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

  Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

  Esta opción está deshabilitada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Categorías de actualizaciones**, seleccione las categorías de actualizaciones que se instalarán. Las categorías son las mismas que se usan en el Catálogo de Microsoft Update. Por defecto, están seleccionadas todas las categorías.

6. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas llegue a su fin, se agregará la nueva regla. La encontrará en la lista de reglas del Asistente para crear nueva tarea o en las propiedades de la tarea.

Para agregar una nueva regla para actualizaciones de aplicaciones de terceros, haga lo siguiente:

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para las actualizaciones de terceros**.

3. En la página **Criterios generales**, defina los siguientes ajustes:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deban instalarse en los dispositivos cliente:

     - **Instalar las actualizaciones aprobadas únicamente**. Solo se instalarán las actualizaciones que estén aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Se instalarán las actualizaciones que tengan el estado de aprobación *Aprobada* o *Sin definir*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Se instalarán todas las actualizaciones, sin importar su estado de aprobación. Tenga cuidado al utilizar esta opción. Selecciónela si, por ejemplo, quiere usar una infraestructura de prueba para evaluar la instalación de algunas actualizaciones rechazadas.

   - Reparar vulnerabilidades que tengan o superen este nivel de gravedad

     Algunas actualizaciones de software pueden afectar negativamente la experiencia de uso de una aplicación. En tales casos, posiblemente quiera instalar solo las actualizaciones que sean fundamentales para el funcionamiento del software y omitir las demás.

     Si esta opción está habilitada, las actualizaciones repararán solo aquellas vulnerabilidades que Kaspersky haya catalogado con un nivel de gravedad igual o superior al valor seleccionado en la lista (**Medio**, **Alto** o **Crítico**). Las vulnerabilidades con un nivel de gravedad inferior al seleccionado no se repararán.

     Si deja esta opción deshabilitada, las actualizaciones repararán todas las vulnerabilidades, sin importar su nivel de gravedad.

     Esta opción está deshabilitada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desee instalar actualizaciones. Por defecto, están seleccionadas todas las aplicaciones.

5. En la página **Nombre**, escriba un nombre para la regla que está agregando. Podrá cambiar este nombre más tarde, en la sección Configuración de la ventana de propiedades de la tarea creada.

Cuando el Asistente de creación de reglas llegue a su fin, se agregará la nueva regla. La encontrará en la lista de reglas del Asistente para crear nueva tarea o en las propiedades de la tarea.

Ver información sobre las vulnerabilidades de software detectadas en todos los dispositivos administrados

Si ya ha analizado el software de los dispositivos administrados en busca de vulnerabilidades, puede ver la lista de vulnerabilidades de software detectadas en la totalidad de los dispositivos administrados. Si ejecuta la tarea para la jerarquía de Servidores de administración, puede ver la lista de dispositivos administrados con vulnerabilidades detectadas solo para el Servidor de administración seleccionado.

Para ver la lista de vulnerabilidades de software detectadas en todos los dispositivos administrados:

En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.

La página muestra la lista de vulnerabilidades de software detectadas en los dispositivos cliente.

También puede generar y ver un informe de vulnerabilidades.

Puede aplicar un filtro para ver la lista de vulnerabilidades de software. Para definir el filtro, haga clic en el ícono **Filtrar** ( ) ubicado en la esquina superior derecha de la lista de vulnerabilidades de software. También puede elegir un filtro preestablecido de la lista desplegable **Filtros preestablecidos**, que se encuentra sobre la lista de vulnerabilidades de software.

Si lo desea, puede obtener información detallada sobre cualquiera de las vulnerabilidades de la lista.

Para obtener información sobre una vulnerabilidad de software:

En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de su interés.

Se abre la ventana de propiedades de la vulnerabilidad de software.

Ver información sobre las vulnerabilidades de software detectadas en un dispositivo administrado específico

Puede ver información sobre las vulnerabilidades de software detectadas en un dispositivo administrado específico que ejecute Windows.

Para ver la lista de las vulnerabilidades de software detectadas en el dispositivo administrado seleccionado:

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

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo para el que desee ver las vulnerabilidades de software detectadas.

   Se muestra la ventana de propiedades del dispositivo seleccionado.

3. En la ventana de propiedades del dispositivo seleccionado, elija la pestaña **Avanzado**.

4. En el panel izquierdo, seleccione la sección **Vulnerabilidades de software**.

Se muestra la lista de vulnerabilidades de software detectadas en el dispositivo administrado que seleccionó.

Para ver las propiedades de una vulnerabilidad de software específica:

En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de software que sea de su interés.

Se muestra la ventana de propiedades de la vulnerabilidad de software seleccionada.

Ver estadísticas de las vulnerabilidades presentes en los dispositivos administrados

Puede ver estadísticas sobre cada vulnerabilidad de software detectada en los dispositivos administrados. Las estadísticas se presentan en forma de diagrama. El diagrama muestra la cantidad de dispositivos con los siguientes estados:

- *Ignorada en: <cantidad de dispositivos>*. Este estado se asigna cuando la vulnerabilidad se desestima manualmente a través de sus propiedades.
- *Reparada en: <cantidad de dispositivos>*. Este estado se asigna cuando la tarea para reparar la vulnerabilidad se completa correctamente.
- *Reparación programada para: <cantidad de dispositivos>*. Este estado se asigna cuando ya se ha creado una tarea para reparar la vulnerabilidad, pero aún no se la ha ejecutado.
- *Parche aplicado en: <cantidad de dispositivos>*. Este estado se asigna cuando se seleccionó manualmente una actualización de software que debía, pero no pudo, reparar la vulnerabilidad.
- *Es necesario realizar un arreglo en: <cantidad de dispositivos>*. Este estado se asigna cuando la vulnerabilidad se ha reparado solo en algunos dispositivos administrados y aún debe repararse en más dispositivos administrados.

Para ver las estadísticas de una vulnerabilidad en los dispositivos administrados:

1. En el menú principal, vaya a **Operaciones → Administración de parches → Vulnerabilidades de software**.

   La página muestra una lista con las vulnerabilidades detectadas en las aplicaciones de los dispositivos administrados.

2. Active la casilla de verificación ubicada junto a la vulnerabilidad de su interés.

3. Haga clic en el botón **Estadísticas de la vulnerabilidad en los dispositivos**.

   Se muestra un diagrama con los estados de la vulnerabilidad. Para ver los dispositivos en los que la vulnerabilidad tenga un estado en particular, haga clic en ese estado.

Exportar la lista de vulnerabilidades de software a un archivo

Puede exportar la lista de vulnerabilidades que se muestra en la aplicación a un archivo CSV o TXT. Una vez que tenga el archivo, podrá almacenarlo para fines estadísticos, enviarlo a la persona que esté a cargo de la seguridad de la información o utilizarlo para otros fines.

Para exportar a un archivo de texto la lista de vulnerabilidades de software detectadas en todos los dispositivos administrados:

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.

   La página muestra una lista con las vulnerabilidades detectadas en las aplicaciones de los dispositivos administrados.

2. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera.

El archivo con la lista de vulnerabilidades de software se guardará en el dispositivo que esté utilizando.

Para exportar a un archivo de texto la lista de vulnerabilidades de software detectadas en un dispositivo administrado específico:

1. Abra la lista de vulnerabilidades de software detectadas en el dispositivo administrado de su interés.

2. Seleccione las vulnerabilidades de software que desee exportar.

   Omita este paso si desea exportar toda la lista de vulnerabilidades de software detectadas en el dispositivo administrado.

   Si desea exportar la lista completa de vulnerabilidades de software detectadas en el dispositivo administrado, tenga en cuenta que solo se exportarán las vulnerabilidades enumeradas en la página que esté viendo.

3. Haga clic en el botón **Exportar a TXT** o en el botón **Exportar a CSV**, dependiendo del formato de exportación que prefiera.

En el dispositivo que esté utilizando, se guardará un archivo con la lista de vulnerabilidades de software detectadas en el dispositivo administrado que haya seleccionado.

Ignorar vulnerabilidades de software

Puede ignorar las vulnerabilidades de software que no desee reparar. Hay distintos motivos para ignorar una vulnerabilidad de software, por ejemplo:

- no considera que la vulnerabilidad de software sea de extrema importancia para su organización;
- entiende que, al reparar la vulnerabilidad, se pondrían en riesgo los datos vinculados al software vulnerable;
- sabe que la vulnerabilidad de software no es un riesgo para la red de su organización porque utiliza otras medidas para proteger sus dispositivos administrados.

Puede ignorar una vulnerabilidad de software en todos los dispositivos administrados o solo en los dispositivos administrados que usted seleccione.

Para ignorar una vulnerabilidad de software en todos los dispositivos administrados:

1. En el menú principal, vaya a **Operaciones** → **Administración de parches** → **Vulnerabilidades de software**.

   La página muestra una lista con las vulnerabilidades de software detectadas en los dispositivos administrados.

2. En la lista de vulnerabilidades de software, haga clic en el vínculo con el nombre de la vulnerabilidad de software que desee ignorar.

   Se abre la ventana de propiedades de la vulnerabilidad de software.

3. En la pestaña **General**, habilite la opción **Ignorar vulnerabilidad**.

4. Haga clic en el botón **Guardar**.

   Se cierra la ventana de propiedades de la vulnerabilidad de software.

La vulnerabilidad de software se ignorará en todos los dispositivos administrados.

Para ignorar una vulnerabilidad de software en un dispositivo administrado específico:

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

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo en el que desee ignorar la vulnerabilidad de software.

   Se abre la ventana de propiedades del dispositivo.

3. En la ventana de propiedades del dispositivo, seleccione la pestaña **Avanzado**.

4. En el panel izquierdo, seleccione la sección **Vulnerabilidades de software**.

   Se muestra la lista de vulnerabilidades de software detectadas en el dispositivo.

5. En la lista de vulnerabilidades de software, seleccione la vulnerabilidad que desee ignorar en el dispositivo seleccionado.

   Se abre la ventana de propiedades de la vulnerabilidad de software.

6. En la ventana de propiedades de la vulnerabilidad de software, en la pestaña **General**, habilite la opción **Ignorar vulnerabilidad**.

7. Haga clic en el botón **Guardar**.

   Se cierra la ventana de propiedades de la vulnerabilidad de software.

8. Cierre la ventana de propiedades del dispositivo.

La vulnerabilidad de software se ignorará en el dispositivo seleccionado.

Cuando se completen las tareas *Reparar vulnerabilidades* o *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las vulnerabilidades de software ignoradas no se repararán. Las vulnerabilidades ignoradas pueden excluirse de la lista de vulnerabilidades utilizando un filtro.

Escenario: Buscar y reparar 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 buscar y reparar vulnerabilidades de software en el sistema operativo y en las aplicaciones de terceros, incluidas las de Microsoft.

Requisitos previos

- Kaspersky Security Center Cloud Console está desplegado 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. **Buscar 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 listas con las vulnerabilidades detectadas y las actualizaciones requeridas para el software de terceros que se encuentra instalado en los dispositivos indicados en las propiedades de la tarea.

   La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente al utilizar el asistente de inicio rápido de Kaspersky Security Center Cloud Console. Si no ejecutó el asistente de inicio rápido, hágalo ahora o cree la tarea manualmente.

   Instrucciones: 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. Puede usar esta tarea para instalar múltiples actualizaciones y reparar múltiples vulnerabilidades utilizando un conjunto de reglas. La disponibilidad de esta tarea depende del modo de Kaspersky Security Center Cloud Console y de la licencia que se está utilizando. Para corregir las vulnerabilidades que se detecten en las aplicaciones, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* usará las actualizaciones de software recomendadas.

   Puede usar la tarea *Reparar vulnerabilidades* para instalar las reparaciones recomendadas para el software de Microsoft.

   Puede crear estas tareas en forma manual o a través de Asistente de reparación de vulnerabilidades, que las crea en forma automática.

   Instrucciones: Reparar 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 creó la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede programarla para que se ejecute con igual o menor frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando defina una programación para la tarea *Reparar vulnerabilidades*, tenga en cuenta que, antes de cada ejecución, deberá seleccionar los parches que se aplicarán al software de Microsoft.

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 vulnerabilidades de software

6. **Ejecutar la 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**

   Controle lo siguiente:

   - La lista de vulnerabilidades de software detectadas en los dispositivos administrados no está vacía.
   - La lista de tareas contiene una tarea de reparación de vulnerabilidades.
   - Las tareas de búsqueda y de reparación de vulnerabilidades están programadas para iniciarse secuencialmente. Para verificar esto, abra las propiedades de las tareas y compare sus programaciones.
   - La tarea de reparación de vulnerabilidades se completó sin inconvenientes. Para verificar esto, revise la información disponible en la pestaña **Resultados** de la ventana de 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. Las actualizaciones de software que cumplen con los criterios especificados en las reglas se descargan en los repositorios de los puntos de distribución y se instalan 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 tiempo máximo por el que la base de datos conservará información sobre las vulnerabilidades reparadas.

   De manera predeterminada, el período de almacenamiento máximo es de 7 días en modo de prueba y de 60 días en modo comercial. El límite absoluto es de 14 días en modo de prueba y de 365 días en 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

En esta sección, se describen las características que Kaspersky Security Center Cloud Console ofrece para administrar las aplicaciones que se ejecutan en los dispositivos cliente.

Uso de Control de aplicaciones para administrar archivos ejecutables

Puede utilizar el componente Control de aplicaciones para permitir o bloquear el inicio de archivos ejecutables en los dispositivos del usuario. El componente Control de aplicaciones es compatible con sistemas operativos Windows y Linux.

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 desplegado 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 para usar el componente Control de aplicaciones se divide 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 visualizar una lista de archivos ejecutables almacenados en los dispositivos cliente

2. **Crear categorías para los archivos ejecutables que se usan en su organización**

   Analice las listas de aplicaciones y archivos ejecutables almacenados en los dispositivos administrados. Cree las categorías para archivos ejecutables en función del análisis. Recomendamos crear una categoría llamada "Aplicaciones de trabajo" que cubra los archivos ejecutables estándar que se utilicen en la organización. Luego, si tiene grupos de seguridad diferentes que trabajan con sus propios archivos ejecutables, puede crear una categoría independiente para cada grupo de seguridad.

   Instrucciones: Crear una categoría de aplicaciones con contenido agregado manualmente, Crear una categoría de aplicaciones 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 creó en la etapa anterior.

   Instrucciones: Configurar 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 necesiten para trabajar. Para asegurarse de que esto sea así, cuando cree nuevas reglas de Control de aplicaciones, recomendamos que habilite un modo de prueba y analice el funcionamiento de las reglas. Mientras este modo esté habilitado, 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 que tales archivos se iniciaron.

   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: Configurar el componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y habilite 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: Agregar archivos ejecutables relacionados con un evento a una categoría de aplicaciones

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: Configurar el componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y deshabilite el modo de prueba en el proceso de configuración.

7. **Verificar la configuración de Control de aplicaciones**

   Controle 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. Revise los ajustes de la directiva de Kaspersky Endpoint Security para Windows y verifique que el componente Control de aplicaciones esté configurado en **Configuración de la aplicación → Controles de seguridad → Control de aplicaciones**.

- Las reglas de Control de aplicaciones se aplican en modo de funcionamiento normal. Busque el modo activo en la directiva de Kaspersky Endpoint Security para Windows; asegúrese de que el **Modo de prueba** esté deshabilitado en **Configuración de la aplicación** → **Controles de seguridad** → **Control de aplicaciones**.

Resultados

Al concluir este procedimiento, el inicio de archivos ejecutables en los dispositivos administrados estará bajo su control. Los usuarios pueden iniciar solo aquellos archivos ejecutables que están permitidos en su organización y no pueden iniciar los que están prohibidos.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux

Modos y categorías de Control de aplicaciones

El componente Control de aplicaciones supervisa los intentos de los usuarios de iniciar archivos ejecutables. Puede usar las reglas de Control de aplicaciones para controlar el inicio de archivos ejecutables.

El componente Control de aplicaciones está disponible para Kaspersky Endpoint Security para Windows y Kaspersky Endpoint Security for Linux (versión 11.2 y posteriores). Las instrucciones de esta sección describen la configuración de Control de aplicaciones para Kaspersky Endpoint Security.

El inicio de archivos ejecutables cuya configuración no coincide con ninguna de las reglas de Control de aplicaciones está regulado por el modo de funcionamiento seleccionado del componente:

- *Lista de rechazados*. En este modo, se permite la ejecución de cualquier archivo ejecutable, excepto los que se especifican en las reglas de bloqueo. El modo *Lista de rechazados* está seleccionado de manera predeterminada.
- *Lista de admitidos*. En este modo, se impide la ejecución de todos los archivos ejecutables, excepto los que se especifican en las reglas de autorización.

Las reglas de Control de aplicaciones se implementan en todas las categorías de archivos ejecutables. En Kaspersky Security Center 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, haga lo siguiente:

En el menú principal, vaya a **Dispositivos** → **Dispositivos administrados** → **<device name>** → **Avanzado** → **Registro de aplicaciones**. En este menú, puede exportar la lista de aplicaciones a un archivo CSV o TXT.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux

Obtener y ver una lista de archivos ejecutables instalados en los dispositivos cliente

Puede obtener la lista de archivos ejecutables almacenados en los dispositivos cliente de una de las siguientes maneras:

- Habilitando las notificaciones sobre el inicio de aplicaciones en la directiva de Kaspersky Endpoint Security.

- Creando una tarea de inventario.

Habilitando las notificaciones sobre el inicio de aplicaciones en la directiva de Kaspersky Endpoint Security

Para habilitar las notificaciones sobre la ejecución de aplicaciones:

1. Abra la configuración de la directiva de Kaspersky Endpoint Security y luego vaya a **Configuración general** → **Informes y almacenamiento**.
2. En el grupo de configuración **Transferencia de datos al servidor de administración**, seleccione la casilla de verificación **Acerca de las aplicaciones iniciadas** y guarde los cambios.

Cuando un usuario intenta iniciar archivos ejecutables, la información sobre estos archivos se añade a la lista de archivos ejecutables en el dispositivo cliente. Kaspersky Endpoint Security envía esta información al Agente de red, que a su vez la envía al Servidor de administración.

Crear una tarea de inventario

La función de inventario de archivos ejecutables está disponible para las siguientes aplicaciones:

- Kaspersky Endpoint Security para Windows
- Kaspersky Endpoint Security for Linux (versión 11.2 y posteriores)

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 **Agregar**.

   Se inicia el Asistente para crear nueva tarea. Siga los pasos del asistente.
3. En la página **Configuración de tarea nueva**, en la lista desplegable **Aplicación**, elija Kaspersky Endpoint Security para Windows o Kaspersky Endpoint Security for Linux, según el tipo de sistema operativo de los dispositivos cliente.
4. En la lista desplegable **Tipo de tarea**, seleccione **Inventario**.
5. En la página **Finalizar la creación de la tarea**, haga clic en el botón **Finalizar**.

Una vez que 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 para Linux

Una vez efectuada la tarea **Inventario**, se crea la lista de archivos ejecutables instalados en los dispositivos administrados para que pueda verla.

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

Para ver la lista de archivos ejecutables almacenados en los dispositivos cliente:

En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Archivos ejecutables**.

La página muestra una lista con los archivos ejecutables instalados en los 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 **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 **Agregar**.

   Se inicia el Asistente para crear nueva categoría. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

3. En el paso **Seleccione un método para crear la categoría**, seleccione la opción **Categoría con contenido agregado de forma manual. Los datos de los archivos ejecutables se agregan de forma manual a la categoría**.

4. En el paso **Condiciones**, haga clic en el botón **Agregar** para agregar un criterio de condición e incluir archivos en la categoría de creación.

5. En el paso **Criterios de la condición**, seleccione el tipo de regla que desee usar para crear la categoría:

   - De la categoría KL

     Seleccione esta opción si, como condición para agregar aplicaciones a la categoría personalizada, desea elegir una categoría de aplicaciones de Kaspersky. Las aplicaciones que pertenezcan a la categoría de Kaspersky elegida se agregarán a la categoría de aplicaciones personalizada.

   - Seleccionar el certificado del repositorio

     Seleccione esta opción para elegir certificados almacenados en el repositorio. La condición de la categoría solo coincide con los archivos ejecutables que están firmados por el certificado especificado.

   - Especificar la ruta a la aplicación (se pueden usar máscaras)

     Seleccione esta opción para especificar la ruta a un archivo o carpeta del dispositivo cliente que contenga los archivos ejecutables que quiera agregar a la categoría de aplicaciones personalizada. Puede utilizar expresiones regulares como *C:\path_to_exe*.*, por ejemplo: *C:\Program Files\Internet Explorer*.*

   - Unidad extraíble

     Seleccione esta opción para especificar el tipo de soporte (unidad extraíble o cualquier tipo de unidad) desde el que se ejecuta la aplicación. Las aplicaciones que se inicien desde el tipo de unidad seleccionado se agregarán a la categoría de aplicaciones personalizada.

   - **Hash, metadatos o certificado**:

     - Seleccionar de la lista de archivos ejecutables

       Seleccione esta opción si desea elegir las aplicaciones que se agregarán a la categoría de la lista de archivos ejecutables almacenados en el dispositivo cliente.

     - Seleccionar del registro de aplicaciones

Si selecciona esta opción, se abrirá el registro de aplicaciones. Después de seleccionar una aplicación del registro, se abre la ventana con los parámetros llenos de metadatos de la aplicación que seleccionó:

- Nombre del archivo.
- Versión del archivo. Puede indicar el número de versión exacto o introducir una condición, como "superior a 5.0".
- Nombre de la aplicación.
- Versión de la aplicación. Puede indicar el número de versión exacto o introducir una condición, como "superior a 5.0".
- Proveedor.

Tenga en cuenta que solo se bloquea la ejecución de archivos ejecutables que cumplan con los parámetros especificados, no la ejecución de la aplicación que seleccione. Si los metadatos de la aplicación seleccionada coinciden con el del archivo ejecutable que se ejecuta al iniciar la aplicación, puede continuar con el siguiente paso. De lo contrario, debe cambiar los valores manualmente para que coincidan con los metadatos del archivo ejecutable.

- Especificar manualmente

Selecciona esta opción para especificar los metadatos, el certificado o el hash de archivo que se tomarán como condición para agregar aplicaciones a la categoría personalizada.

Hash de archivo

Dependiendo de la versión de la aplicación de seguridad instalada en los dispositivos de su red, deberá seleccionar el algoritmo que Kaspersky Security Center Cloud Console usará para calcular el valor hash de los archivos de la categoría. La información sobre los valores hash calculados por las funciones hash se almacena en la base de datos del Servidor de administración.

SHA256 es una función de hash criptográfica. En la actualidad, se la considera la más confiable en su clase, pues no se encontró vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security puede calcular hashes SHA256 desde la versión 10 Service Pack 2 para Windows. Las versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows son compatibles con la función de hash MD5.

Seleccione cualquiera de estas opciones para que Kaspersky Security Center Cloud Console calcule el valor hash de los archivos agregados a la categoría:

- Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores, marque la casilla **SHA256**. Si hay versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows en su red, recomendamos que no agregue categorías que utilicen como criterio el hash SHA256 del archivo ejecutable. Si lo hace, la aplicación de seguridad podría no funcionar correctamente. De presentarse inconvenientes, utilice la función de hash criptográfico MD5 para los archivos de la categoría.

- Si hay alguna versión anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows instalada en su red, seleccione **Hash MD5**. No puede agregar una categoría que se haya creado según el criterio de la suma de verificación MD5 de un archivo ejecutable para Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores. De presentarse inconvenientes, utilice la función de hash criptográfico SHA256 para los archivos de la categoría.

- Si diferentes dispositivos en su red usan versiones anteriores y posteriores de Kaspersky Endpoint Security 10, marque la casilla **SHA256** y la casilla **Hash MD5**.

Metadatos

Seleccione esta opción si desea especificar los metadatos de los archivos (nombre, versión, proveedor, etc.). La condición de la categoría solo coincide con los archivos ejecutables que tienen los mismos metadatos.

Certificado

Seleccione esta opción para elegir certificados almacenados en el repositorio. La condición de la categoría solo coincide con los archivos ejecutables que están firmados por el certificado especificado.

- Desde archivo o paquete MSI/carpeta archivada

Seleccione esta opción para especificar un archivo de instalador MSI como condición para agregar aplicaciones a la categoría personalizada. Los metadatos del instalador se enviarán al Servidor de administración. Las aplicaciones que tengan los mismos metadatos de instalador que el instalador MSI especificado se agregarán a la categoría de aplicaciones personalizada.

El criterio seleccionado se agrega a la lista de condiciones.

Puede agregar tantos criterios como necesite para crear la categoría de aplicaciones.

6. En el paso **Exclusiones**, haga clic en el botón **Agregar** para agregar un criterio de condición excluyente que permita excluir archivos de la nueva categoría.

7. En el paso **Criterios de la condición**, seleccione un tipo de regla tal como lo hizo al elegir un tipo de regla para crear la categoría.

Cuando el asistente finaliza, se crea la categoría de aplicaciones. La nueva categoría aparece en la lista de categorías de aplicaciones. Podrá usar la nueva categoría cuando configure Control de aplicaciones.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux

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 **Agregar**.

   Se inicia el Asistente para crear nueva categoría. Utilice el botón **Next** para avanzar a un nuevo paso del asistente.

3. En el paso **Seleccione un método para crear la categoría**, especifique el nombre para la categoría y seleccione la opción **Categoría que incluye los archivos ejecutables de los dispositivos seleccionados. Estos archivos ejecutables se procesan de forma automática y sus métricas se agregan a la categoría**.

4. Haga clic en **Agregar**.

5. En la ventana que se abre, seleccione el dispositivo que contenga los archivos ejecutables que desee usar para crear la categoría. Puede seleccionar más de un dispositivo.

6. Configure los siguientes ajustes:

   - Algoritmo de evaluación del valor de hash

Dependiendo de la versión de la aplicación de seguridad instalada en los dispositivos de su red, deberá seleccionar el algoritmo que Kaspersky Security Center Cloud Console usará para calcular el valor hash de los archivos de la categoría. La información sobre los valores hash calculados por las funciones hash se almacena en la base de datos del Servidor de administración.

SHA256 es una función de hash criptográfica. En la actualidad, se la considera la más confiable en su clase, pues no se encontró vulnerabilidad alguna en su algoritmo. Kaspersky Endpoint Security puede calcular hashes SHA256 desde la versión 10 Service Pack 2 para Windows. Las versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows son compatibles con la función de hash MD5.

Seleccione cualquiera de estas opciones para que Kaspersky Security Center Cloud Console calcule el valor hash de los archivos agregados a la categoría:

- Si todas las instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores, marque la casilla **SHA256**. Si hay versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows en su red, recomendamos que no agregue categorías que utilicen como criterio el hash SHA256 del archivo ejecutable. Si lo hace, la aplicación de seguridad podría no funcionar correctamente. De presentarse inconvenientes, utilice la función de hash criptográfico MD5 para los archivos de la categoría.

- Si hay alguna versión anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows instalada en su red, seleccione **Hash MD5**. No puede agregar una categoría que se haya creado según el criterio de la suma de verificación MD5 de un archivo ejecutable para Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores. De presentarse inconvenientes, utilice la función de hash criptográfico SHA256 para los archivos de la categoría.

Si diferentes dispositivos en su red usan versiones anteriores y posteriores de Kaspersky Endpoint Security 10, marque la casilla **SHA256** y la casilla **Hash MD5**.

La casilla **Calcular SHA256 para los archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores)** está activada de manera predeterminada.

De manera predeterminada, la casilla **Calcular MD5 para los archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)** está desactivada.

- Sincronizar datos con el repositorio del Servidor de administración

Seleccione esta opción si desea que el Servidor de administración verifique periódicamente si ha habido cambios en la(s) carpeta(s) especificada(s).

Esta opción está deshabilitada de forma predeterminada.

Si habilita esta opción, indique la frecuencia (en horas) con la que se llevará a cabo la verificación. Por defecto, se realiza una búsqueda de cambios cada veinticuatro horas.

- Tipo de archivo

Utilice esta sección para especificar qué clase de archivos se usarán para crear la categoría de aplicaciones.

Todos los archivos. Para crear la categoría, se tendrán en cuenta todos los archivos. Esta opción está seleccionada de forma predeterminada.

Solo archivos fuera de las categorías de aplicaciones. Para crear la categoría, solo se tendrán en cuenta los archivos que no estén incluidos en las categorías de aplicaciones.

- **Carpetas**

  Utilice esta sección para elegir las carpetas del dispositivo (o de los dispositivos) que contengan los archivos que se usarán para crear la categoría de aplicaciones.

  Todas las carpetas. Para crear la categoría, se tendrán en cuenta todas las carpetas. Esta opción está seleccionada de forma predeterminada.

  Carpeta especificada: Para crear la categoría, solo se tendrá en cuenta la carpeta especificada. Si selecciona esta opción, deberá especificar la ruta a la carpeta.

Cuando finaliza el asistente, se crea la categoría para archivos ejecutables. se muestra en la lista de categorías. Podrá usar la categoría creada cuando configure Control de aplicaciones.

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 de **Kaspersky Endpoint Security para Windows**.

   Se abre la ventana de configuración de la directiva.

3. Vaya a **Configuración de la aplicación → Controles de seguridad → Control de aplicaciones**.

   Se abre la ventana **Control de aplicaciones**, en la que encontrará los ajustes de Control de aplicaciones.

4. La opción **Control de aplicaciones** está habilitada de manera predeterminada. Pase el interruptor a **Control de aplicaciones DESHABILITADO** para deshabilitar la opción.

5. En el bloque de opciones **Configuración de Control de aplicaciones**, habilite el modo de funcionamiento pertinente para aplicar las reglas de Control de aplicaciones y permitir que Kaspersky Endpoint Security para Windows bloquee el inicio de aplicaciones.

   Si desea probar las reglas de Control de aplicaciones, en la sección **Configuración de Control de aplicaciones**, habilite el modo de prueba. Cuando el modo de prueba está habilitado, Kaspersky Endpoint Security para Windows no bloquea el inicio de las aplicaciones, pero registra información sobre las reglas activadas en el informe. Haga clic en el vínculo **Ver informe** para ver esa información.

6. Habilite la opción **Controlar la carga de módulos DLL** si desea que Kaspersky Endpoint Security para Windows monitoree la carga de módulos DLL cuando los usuarios inicien aplicaciones.

   Se guardará un informe con datos sobre los módulos y sobre las aplicaciones que carguen esos módulos.

   Kaspersky Endpoint Security para Windows únicamente atenderá a los módulos DLL y controladores que se carguen después de que habilite la opción **Controlar la carga de módulos DLL**. Reinicie el equipo tras habilitar la opción **Controlar la carga de módulos DLL** si desea que Kaspersky Endpoint Security para Windows monitoree la carga de todos los módulos DLL y controladores, incluidos aquellos que se carguen antes de la ejecución de Kaspersky Endpoint Security para Windows.

7. (Opcional). En el bloque **Plantillas de mensajes**, modifique la plantilla del mensaje que se le muestra al usuario cuando se le impide iniciar una aplicación y la plantilla del correo electrónico que el usuario le puede enviar a usted.

8. En el bloque de opciones **Modo de Control de aplicaciones**, seleccione el modo **Lista de rechazados** o el modo **Lista de admitidos**.

   De forma predeterminada, está seleccionado el modo **Lista de rechazados**.

9. Haga clic en el vínculo **Configuración de las listas de reglas**.

   Se abre la ventana **Listas de rechazados y admitidos** que permite agregar una categoría de aplicaciones. De manera predeterminada, la pestaña **Lista de rechazados** está seleccionada si se selecciona el modo **Lista de rechazados**, o la pestaña **Lista de admitidos** si se selecciona el modo **Lista de admitidos**.

10. En la ventana **Listas de rechazados y admitidos**, haga clic en el botón **Agregar**.

    Se abre la ventana **Regla de Control de aplicaciones**.

11. Haga clic en el vínculo **Debe elegir una categoría**.

    Se abre la ventana **Categoría de aplicaciones**.

12. Agregue la categoría de aplicaciones (o las categorías de aplicaciones) que creó anteriormente.

    Si desea modificar la configuración de una categoría que creó, haga clic en el botón **Editar**.

    Si desea crear una nueva categoría, haga clic en el botón **Agregar**.

    Si desea eliminar una categoría de la lista, haga clic en el botón **Eliminar**.

13. Una vez que la lista de categorías de aplicaciones esté completa, haga clic en el botón **Aceptar**.

    Se cierra la ventana **Categoría de aplicaciones**.

14. En la ventana de la regla de **Control de aplicaciones**, en la sección **Usuarios y sus derechos**, cree una lista con los usuarios y grupos de usuarios a los que se aplicará la regla de Control de aplicaciones.

15. Haga clic en el botón **Aceptar** para guardar la configuración y cerrar la ventana **Regla de Control de aplicaciones**.

16. Haga clic en el botón **Aceptar** para guardar la configuración y cerrar la ventana **Listas de rechazados y admitidos**.

17. Haga clic en el botón **Aceptar** para guardar la configuración y cerrar la ventana **Control de aplicaciones**.

18. Cierre la ventana con la configuración de la directiva de Kaspersky Endpoint Security para Windows.

    Se guarda la configuración de Control de aplicaciones. Una vez que la directiva se propague a los dispositivos cliente, el inicio de archivos ejecutables estará bajo su control.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux

Agregar archivos ejecutables vinculados a eventos a una categoría de aplicaciones

Una vez que configure el componente Control de aplicaciones en las directivas de Kaspersky Endpoint Security para Windows, podrá ver los siguientes eventos en la lista de eventos:

- **Inicio de aplicación prohibido** (evento de nivel *Crítico*). Este evento se muestra si Control de aplicaciones se ha configurado para hacer cumplir sus reglas.
- **Inicio de aplicación prohibido en el modo de prueba** (evento de nivel *Información*). Este evento se muestra si Control de aplicaciones se ha configurado para aplicar sus reglas en modo de prueba.
- **Mensaje para el administrador sobre la prohibición de inicio de la aplicación** (*evento de Advertencia*). Este evento aparece si Control de aplicaciones se ha configurado para hacer cumplir sus reglas y un usuario ha solicitado acceso a una aplicación que no tiene permitido ejecutar.

Recomendamos crear selecciones de eventos para ver los eventos relacionados con el funcionamiento de Control de aplicaciones.

Puede agregar los archivos ejecutables vinculados a los eventos de Control de aplicaciones a una categoría de aplicaciones nueva o existente. En cualquiera de los dos casos, la categoría debe ser una categoría de aplicaciones con contenido agregado manualmente.

Para agregar archivos ejecutables vinculados a los eventos de Control de aplicaciones a una categoría de aplicaciones:

1. En el menú principal, vaya a **Supervisión e informes → Selecciones de eventos**.

   Se muestra la lista de selecciones de eventos.

2. Elija y genere una selección de eventos que le permita ver los eventos relacionados con Control de aplicaciones.

   Si no creó una selección de eventos relacionada con Control de aplicaciones, puede seleccionar y generar una de las selecciones predefinidas (por ejemplo, **Eventos recientes**).

   Se muestra la lista de eventos.

3. Seleccione los eventos asociados a los archivos ejecutables que desee agregar a la categoría de aplicaciones. A continuación, haga clic en el botón **Asignar a categoría**.

   Se inicia el Asistente para crear nueva categoría. Utilice el botón **Next** para avanzar a un nuevo paso del asistente.

4. En la página del asistente, configure los ajustes pertinentes:

   - En la sección **Acción sobre archivo ejecutable relacionado con el evento**, seleccione una de las siguientes opciones:

     - Agregar a una nueva categoría de aplicación

       Seleccione esta opción si desea crear una nueva categoría de aplicaciones basada en los archivos ejecutables vinculados a los eventos.

       Esta opción está seleccionada de forma predeterminada.

       Si selecciona esta opción, escriba el nombre que tendrá la nueva categoría.

     - Agregar a una categoría de aplicación existente

       Seleccione esta opción si desea agregar los archivos ejecutables vinculados a los eventos a una categoría de aplicaciones existente.

       Esta opción no está seleccionada de manera predeterminada.

       Si selecciona esta opción, elija la categoría de aplicaciones con contenido agregado manualmente a la que desee agregar los archivos ejecutables.

   - En la sección **Tipo de reglas**, seleccione una de las siguientes opciones:

     - **Reglas para agregar a inclusiones**
     - **Reglas para agregar a exclusiones**

   - En la sección **Parámetro utilizado como condición**, seleccione una de las siguientes opciones:

     - Detalles del certificado (o hashes SHA256 para archivos sin certificado)

       Los archivos pueden estar firmados con un certificado. Cada certificado puede utilizarse para firmar más de un archivo. Un mismo certificado puede usarse para firmar distintas versiones de una misma aplicación, por ejemplo, o distintas aplicaciones de un mismo proveedor. Cuando seleccione un certificado, podría suceder que la categoría termine con varias versiones de una misma aplicación o con varias aplicaciones de un mismo proveedor.

       Cada archivo tiene su propia función hash SHA256. Si selecciona una función hash SHA256, solo se agregará a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

       Seleccione esta opción si desea agregar los detalles del certificado de un archivo ejecutable (o la función hash SHA256 de los archivos sin certificado) a las reglas de la categoría.

       Esta opción está seleccionada de forma predeterminada.

     - Detalles del certificado (los archivos sin certificado se omitirán)

Los archivos pueden estar firmados con un certificado. Cada certificado puede utilizarse para firmar más de un archivo. Un mismo certificado puede usarse para firmar distintas versiones de una misma aplicación, por ejemplo, o distintas aplicaciones de un mismo proveedor. Cuando seleccione un certificado, podría suceder que la categoría termine con varias versiones de una misma aplicación o con varias aplicaciones de un mismo proveedor.

Seleccione esta opción si desea agregar los detalles del certificado de un archivo ejecutable a las reglas de la categoría. Si el archivo ejecutable no tiene certificado, el archivo se omitirá. No se agregará información sobre ese archivo a la categoría.

- **Solo SHA256 (los archivos sin hash se omitirán)**

  Cada archivo tiene su propia función hash SHA256. Si selecciona una función hash SHA256, solo se 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 SHA256 del archivo ejecutable.

- **Solo MD5 (modo discontinuado, solo para Kaspersky Endpoint Security 10 Service Pack 1)**

  Cada archivo tiene su propia función hash MD5. Si selecciona una función hash MD5, solo se agregará a la categoría el archivo específico que se corresponda con ese hash (por ejemplo, la versión especificada de la aplicación).

  Seleccione esta opción si solo desea agregar los detalles de la función hash MD5 del archivo ejecutable. La capacidad de calcular hashes MD5 está disponible para Kaspersky Endpoint Security 10 Service Pack 1 para Windows y versiones anteriores.

5. Haga clic en **Aceptar**.

Cuando finaliza el asistente, los archivos ejecutables vinculados a los eventos de Control de aplicaciones se agregan a la categoría de aplicaciones nueva o existente. Puede ver la configuración de la categoría de aplicaciones creada o modificada.

Para obtener información detallada sobre el Control de aplicaciones, consulte los siguientes temas de ayuda:

- Ayuda en línea de Kaspersky Endpoint Security para Windows
- Ayuda en línea de Kaspersky Endpoint Security for Linux

Crear un paquete de instalación para una aplicación de terceros usando la base de datos de Kaspersky

Kaspersky Security Center Web Console permite instalar aplicaciones de terceros en forma remota utilizando paquetes de instalación. Las aplicaciones de terceros se incluyen en una base de datos dedicada de Kaspersky.

La creación de paquetes de instalación de aplicaciones de terceros desde la base de datos de Kaspersky solo está disponible con 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 **Descubrimiento y despliegue → Despliegue y asignación → Paquetes de instalación**.
2. Haga clic en el botón **Agregar**.
3. En la página Asistente de nuevo paquete que se abre, seleccione la opción **Seleccionar una aplicación de la base de datos de Kaspersky para crear un paquete de instalación** y luego haga clic en **Siguiente**.
4. En la lista de aplicaciones que se abre, seleccione la aplicación correspondiente y luego haga clic en **Siguiente**.
5. Seleccione el idioma de localización relevante en la lista desplegable y luego haga clic en **Siguiente**.

   Este paso solo se muestra si la aplicación brinda varias opciones de idioma.

6. Si se le solicita que acepte un Acuerdo de licencia para la instalación, en la página **Contrato de licencia de usuario final** que se abre, haga clic en el vínculo para leer el Contrato de licencia en el sitio web del proveedor y luego seleccione la casilla de verificación **Confirmo que he leído completamente, entiendo y acepto los términos y las condiciones de este Contrato de licencia de usuario final**.
7. En la página **Nombre del nuevo paquete de instalación** que se abre, en el campo **Nombre del paquete**, ingrese el nombre del paquete de instalación y luego haga clic en **Siguiente**.

Espere hasta que el paquete de instalación recién creado se cargue en el Servidor de administración. Cuando el Asistente de nuevo paquete muestre el mensaje que le informa que el proceso de creación del paquete se realizó correctamente, haga clic en **Finalizar**.

El paquete de instalación recién creado aparecerá en la lista de paquetes de instalación. Puede seleccionar este paquete al crear o reconfigurar la tarea *Instalar aplicación de forma remota*.

Ver y modificar la configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky

Si creó un paquete de instalación para algunas de las aplicaciones de terceros incluidas en la base de datos de Kaspersky, puede ver y modificar posteriormente la configuración de esto paquete.

La modificación de la configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky solo está disponible con la licencia Administración de vulnerabilidades y parches.

Para ver y modificar la configuración de un paquete de instalación de una aplicación de terceros incluida en la base de datos de Kaspersky:

1. En el menú principal, vaya a **Descubrimiento y despliegue → Despliegue y asignación → Paquetes de instalación**.
2. En la lista de paquetes de instalación que se abre, haga clic en el nombre del paquete pertinente.
3. En la página de propiedades que se abre, modifique la configuración, si es necesario.

4. Haga clic en el botón **Guardar**.

Se guarda la configuración modificada.

Configurar el paquete de instalación de una aplicación de terceros incluida en la base de datos de Kaspersky

La configuración de un paquete de instalación de una aplicación de terceros se agrupa en las siguientes pestañas:

Solo una parte de la configuración que se muestra a continuación se muestra de forma predeterminada, por lo que puede agregar las columnas correspondientes haciendo clic en **Filtrar** y seleccionando los nombres de columna relevantes de la lista.

- Pestaña **General**:
  - Campo de entrada que contiene el nombre del paquete de instalación que se puede editar manualmente
  - Aplicación

    El nombre de la aplicación de terceros para la que se creó el paquete de instalación.
  - Versión

    El número de versión de la aplicación de terceros para la que se creó el paquete de instalación.
  - Tamaño

    El tamaño del paquete de instalación de terceros (en kilobytes).
  - Creado

    La fecha y la hora en que se creó el paquete de instalación de terceros.
  - Ruta

    La ruta a la carpeta de red donde se almacena el paquete de instalación de terceros.
- Pestaña **Procedimiento de instalación**:
  - Instalar los componentes generales obligatorios del sistema

    Si esta opción está habilitada, antes de que se instale una actualización, la aplicación instalará automáticamente todos los componentes generales del sistema que la actualización requiera para instalarse (los llamados "requisitos previos"). Una actualización podría requerir, por ejemplo, que esté instalada cierta actualización del sistema operativo.

    Si esta opción está deshabilitada, posiblemente tenga que instalar los requisitos previos manualmente.

    Esta opción está deshabilitada de forma predeterminada.

- Tabla que muestra las propiedades de actualización y que contiene las siguientes columnas:
  - **Nombre**

    Nombre de la actualización.

  - **Descripción**

    Descripción de la actualización.

  - **Origen**

    El origen de la actualización, es decir, si fue publicada por Microsoft o por un desarrollador externo diferente.

  - **Tipo**

    El tipo de actualización, es decir, si la actualización está destinada a un controlador o una aplicación.

  - **Categoría**

    La categoría de Windows Server Update Services (WSUS) que se muestra para las actualizaciones de Microsoft (Actualizaciones críticas, Actualizaciones de las definiciones, Controladores, Paquetes de características, Actualizaciones de seguridad, Service Packs, Herramientas, Paquetes acumulativos de actualizaciones, Actualizaciones o Upgrade).

  - **Nivel de importancia conforme a MSRC**

    El nivel de importancia de la actualización definido por el Centro de respuesta de seguridad de Microsoft (MSRC).

  - **Nivel de importancia**

    El nivel de importancia de la actualización definido por Kaspersky.

  - **Nivel de importancia del parche**

    El nivel de importancia del parche si está destinado a una aplicación de Kaspersky.

  - **Artículo**

    El identificador (id.) del artículo de la Base de conocimientos que describe la actualización.

  - **Boletín**

    El id. del boletín de seguridad que describe la actualización.

  - **Instalación no asignada (nueva versión)**

    Muestra si la actualización tiene el estado Instalación no asignada.

- **Por instalarse**

  Muestra si la actualización tiene el estado Por instalarse.

- **Instalándose**

  Muestra si la actualización tiene el estado Instalándose.

- **Instalada**

  Muestra si la actualización tiene el estado Instalada.

- **Error**

  Muestra si la actualización tiene el estado Error.

- **Se debe reiniciar el dispositivo**

  Muestra si la actualización tiene el estado Se debe reiniciar el dispositivo.

- **Registrada**

  Muestra la fecha y hora en que se registró la actualización.

- **Instalada en modo interactivo**

  Muestra si la actualización solicita la intervención del usuario durante la instalación.

- **Revocado**

  Muestra la fecha y hora en que se revocó la actualización.

- **Estado de aprobación de la actualización**

  Muestra si la instalación de la actualización está aprobada.

- **Revisión**

  Muestra el número de revisión actual de la actualización.

- **Id. de actualización**

  Muestra el id. de la actualización.

- **Versión de la aplicación**

  Muestra el número de versión a la que se actualizará la aplicación.

- **Reemplazada**

Muestra otras actualizaciones que pueden reemplazar a la actualización.

- **Reemplaza**

  Muestra otras actualizaciones que pueden ser reemplazadas por la actualización.

- **Debe aceptar los términos del Contrato de licencia**

  Muestra si la actualización solicita aceptar los términos de un contrato de licencia de usuario final (EULA).

- **Dirección URL de descripción**

  Muestra el nombre del proveedor de la actualización.

- **Familia de aplicaciones**

  Muestra el nombre de la familia de aplicaciones a las que pertenece la actualización.

- **Aplicación**

  Muestra el nombre de la aplicación a la que pertenece la actualización.

- **Idioma de localización**

  Muestra el idioma de localización de la actualización.

- **Instalación no asignada (nueva versión)**

  Muestra si la actualización tiene el estado Instalación no asignada (nueva versión).

- **Requiere instalación de requisitos previos**

  Muestra si la actualización tiene el estado Requiere instalación de requisitos previos.

- **Modo de descarga**

  Muestra el modo de descarga de la actualización.

- **Es un parche**

  Muestra si la actualización es un parche.

- **Sin instalar**

  Muestra si la actualización tiene el estado Sin instalar.

- Pestaña **Configuración** que muestra la configuración del paquete de instalación (con sus nombres, descripciones y valores) que se utilizan como parámetros de la línea de comandos durante la instalación. Si el paquete no proporciona dicha configuración, se muestra el mensaje correspondiente. Puede modificar los valores de esta configuración.

- Pestaña **Historial de revisiones** que muestra las revisiones del paquete de instalación y que contiene las siguientes columnas:

  - **Revisión**: muestra el número de revisión de los paquetes de instalación.

  - **Hora**: fecha y hora en que se modificó la configuración del paquete de instalación.

  - **Usuario**: nombre del usuario que modificó la configuración del paquete de instalación.

  - **Acción**: acción realizada sobre el paquete de instalación dentro de la revisión.

  - **Descripción**: descripción de la revisión vinculada al cambio realizado en la configuración del paquete de instalación.

    De manera predeterminada, la descripción de las revisiones está en blanco. Para agregar una descripción a una revisión, seleccione la revisión pertinente y haga clic en el botón **Editar descripción**. En la ventana abierta, ingrese un texto que describa la revisión.

Etiquetas de aplicación

Kaspersky Security Center 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 aplicación**.

2. Haga clic en **Agregar**.

   Se abre una ventana para crear la etiqueta.

3. Introduzca el nombre de la etiqueta.

4. Haga clic en **Aceptar** para guardar los cambios.

La nueva etiqueta aparece en la lista de etiquetas de aplicación.

Cambiar el nombre de una etiqueta de aplicación

Para cambiar el nombre de una etiqueta de aplicación:

1. En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Etiquetas de aplicación**.
2. Marque la casilla ubicada junto a la etiqueta a la que desee cambiarle el nombre y haga clic en **Editar**.

   Se abre la ventana de propiedades de la etiqueta.
3. Cambie el nombre de la etiqueta.
4. Haga clic en **Aceptar** para guardar los cambios.

La etiqueta actualizada aparece en la lista de etiquetas de aplicación.

Asignación de etiquetas a una aplicación

Para asignar una o varias etiquetas a una aplicación:

1. En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Registro de aplicaciones**.
2. Haga clic en el nombre de la aplicación a la que desee asignar las etiquetas.
3. Seleccione la pestaña **Etiquetas**.

   En la pestaña, verá todas las etiquetas de aplicación que existan en el Servidor de administración. Las etiquetas que estén asignadas a la aplicación elegida tendrán una casilla activada en la columna **Modo de asignación**.
4. Busque las etiquetas que desee asignar y active las casillas de verificación correspondientes en la columna **Modo de asignación**.
5. Haga clic en **Guardar** para guardar los cambios.

Se asignan las etiquetas a la aplicación.

Quitarle una etiqueta a una aplicación

Para quitarle una o más etiquetas a una aplicación:

1. En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Registro de aplicaciones**.
2. Haga clic en el nombre de la aplicación a la que desee quitarle etiquetas.
3. Seleccione la pestaña **Etiquetas**.

   En la pestaña, verá todas las etiquetas de aplicación que existan en el Servidor de administración. Las etiquetas que estén asignadas a la aplicación elegida tendrán una casilla activada en la columna **Modo de asignación**.

4. Busque las etiquetas que desee quitarle a la aplicación y desactive las casillas de verificación correspondientes en la columna **Modo de asignación**.

5. Haga clic en **Guardar** para guardar los cambios.

Se le quitan las etiquetas seleccionadas a la aplicación.

> Las etiquetas de aplicación desasignadas no se eliminan. Si lo desea, puede eliminarlas manualmente.

Eliminación de una etiqueta de aplicación

Para eliminar una etiqueta de aplicación:

1. En el menú principal, vaya a **Operaciones** → **Aplicaciones de terceros** → **Etiquetas de aplicación**.

2. En la lista, seleccione la etiqueta de aplicación que desee eliminar.

3. Haga clic en el botón **Eliminar**.

4. En la ventana que se abre, haga clic en **Aceptar**.

Se elimina la etiqueta de aplicación. La etiqueta eliminada se borra automáticamente de las aplicaciones a las que estaba asignada.

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 desplegado en su infraestructura local funcione como Servidor de administración secundario y crear, con ello, una jerarquía principal-secundario en su red. Para el Servidor de administración desplegado en la infraestructura de Kaspersky, los servidores de administración principal y secundario ubicados en su red serán servidores secundarios. Puede agregar un Servidor de administración instalado en Windows o un Servidor de administración instalado en Linux.

Para agregar un Servidor de administración secundario con el que se pueda establecer conexión:

1. Asegúrese de que el futuro Servidor de administración secundario tenga Kaspersky Security Center Web Console instalado.

2. En el futuro Servidor de administración secundario, descargue y guarde el certificado del Servidor de administración. Deberá agregar este certificado en el Servidor de administración principal al realizar uno de los pasos del Asistente para agregar un Servidor de administración secundario.

3. Utilice Kaspersky Security Center Web Console para realizar las siguientes acciones en el futuro Servidor de administración secundario (o pídale al administrador del futuro Servidor de administración secundario que realice estas acciones):

   a. En el menú principal, haga clic en el ícono de configuración ( ) ubicado 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 un servidor secundario en la jerarquía**.

   d. Seleccione **Cloud Console** como Servidor de administración principal.

      Se habilitan los campos para configurar los ajustes de la conexión entre los servidores de administración secundario y principal.

   e. En los campos **Dirección del servidor HDS (tomada del Servidor de administración principal en Cloud Console)** y **Puertos del servidor HDS**, ingrese la dirección y el puerto del Servidor de administración principal de Kaspersky Security Center Cloud Console.

      Encontrará la dirección del servidor HDS y el puerto del servidor HDS en la ventana de propiedades del Servidor de administración de Kaspersky Security Center Cloud Console, dentro de la sección **Jerarquía de Servidores de administración** de la pestaña **General**. 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.

      Para descargar este certificado, ingrese a la ventana de propiedades del Servidor de administración de Kaspersky Security Center Cloud Console y, en la sección **Jerarquía de Servidores de administración** de la pestaña **General**, haga clic en el botón **Ver el certificado del Servidor de administración**.

g. Haga clic en el botón **Especificar los certificados de Hosted Discovery Service**, y luego seleccione el certificado.

Para descargar este certificado, ingrese a la ventana de propiedades del Servidor de administración de Kaspersky Security Center Cloud Console y, en la sección **Jerarquía de Servidores de administración** de la pestaña **General**, haga clic en el botón **Certificado de CA raíz de 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), indíquelo e ingrese las credenciales del servidor proxy.

i. Seleccione la opción **Conectar el Servidor de administración principal a un 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 ícono de configuración ( ) ubicado 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. Marque la casilla ubicada junto al nombre del grupo de administración al que desee agregar el Servidor de administración secundario.

7. En la línea del menú, haga clic en **Conectar Servidor de administración secundario**.

Se inicia el Asistente para agregar un Servidor de administración secundario. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.

8. Complete los siguientes campos:

- Nombre para mostrar del Servidor de administración secundario

  Un nombre para identificar al Servidor de administración secundario en la jerarquía. Puede usar, por ejemplo, la dirección IP del Servidor o una frase como "Servidor secundario para el grupo 1".

- Dirección del Servidor de administración secundario (opcional)

  Escriba la dirección IP o el nombre de dominio del Servidor de administración secundario.

  Este parámetro es necesario si la opción **Conectar el Servidor de administración principal al Servidor de administración secundario en DMZ** está habilitada.

9. Si utiliza un servidor proxy para conectarse al Servidor de administración de Kaspersky Security Center Cloud Console (es decir, al futuro Servidor principal), indíquelo e ingrese las credenciales del servidor proxy.

10. Siga las instrucciones adicionales del asistente.

Al concluir el asistente, se creará la jerarquía principal-secundario. El Servidor de administración principal comenzará a recibir conexión del Servidor de administración secundario a través del puerto 13000. Se recibirán y aplicarán las tareas y directivas del Servidor de administración principal. El Servidor de administración secundario aparecerá en el Servidor de administración principal, en el grupo de administración en el que se lo haya agregado.

Configuración del plazo de almacenamiento para eventos vinculados a dispositivos eliminados

En Kaspersky Security Center Cloud Console, los eventos se almacenan en un repositorio de eventos. No es posible configurar la cantidad de eventos que se guardan en el repositorio de eventos.

En la sección **Repositorio de eventos** de la ventana de propiedades del Servidor de administración, puede configurar el plazo de almacenamiento máximo para los eventos vinculados a dispositivos eliminados. El plazo de almacenamiento máximo es de 1000 días.

Para definir por cuántos días se conservarán los eventos relacionados con dispositivos eliminados:

1. En el menú principal, haga clic en el ícono de configuración ( ) ubicado 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 los eventos de los dispositivos eliminados**.

4. En el cuadro de edición **Periodo máximo de almacenamiento (días)**, especifique por cuántos días se almacenarán los eventos vinculados a dispositivos eliminados.

Los eventos vinculados a dispositivos eliminados se almacenarán, como máximo, la cantidad de días indicada.

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.

Combinación de correos electrónicos sobre eventos

Kaspersky Security Center Cloud Console y las aplicaciones de Kaspersky administradas generan eventos cuando están en funcionamiento. A cada evento se le atribuye un tipo y un nivel de gravedad (*Evento crítico*, *Error funcional*, *Advertencia* o *Información*). Si dos eventos de un mismo tipo ocurren en condiciones diferentes, Kaspersky Security Center Cloud Console puede asignarles niveles de gravedad diferentes.

Kaspersky Security Center Cloud Console notifica de los eventos en forma automática, por correo electrónico. Kaspersky Security Center Cloud Console envía notificaciones sobre los eventos que figuran en la pestaña **Configuración de eventos** de la ventana **Propiedades del Servidor de administración**. A la hora de dar aviso de los eventos, se utilizan una serie de opciones de notificación que son comunes a todos los tipos de eventos.

Para limitar el número de correos electrónicos que deben enviarse, Kaspersky Security Center Cloud Console, durante períodos específicos, combina los eventos que comparten un nivel de gravedad. Los especialistas de Kaspersky definen el largo de estos períodos. Como resultado, los destinatarios reciben correos electrónicos combinados basados en la siguiente plantilla: "<Número> eventos de nivel <nivel_de_gravedad> y otros eventos de menor nivel han ocurrido".

Limitaciones para administrar servidores de administración secundarios instalados en una infraestructura local con Kaspersky Security Center Cloud Console

Después de cambiar a un Servidor de administración secundario instalado en una infraestructura local mediante la opción correspondiente de Kaspersky Security Center Cloud Console, la aplicación impondrá limitaciones específicas para administrar ese servidor de administración secundario. El usuario perderá acceso a los siguientes ajustes vinculados al funcionamiento de Kaspersky Security Center Cloud Console:

- En los ajustes de las directivas para el Agente de red y para el Servidor de administración, las pestañas **Configuración de eventos** y **Configuración de la aplicación** dejarán de estar disponibles. No se podrán crear nuevas directivas.
- En los ajustes de las tareas para el Agente de red y para el Servidor de administración, las pestañas **Configuración de eventos** y **Configuración de la aplicación** dejarán de estar disponibles. No se podrán crear nuevas tareas.
- No se podrá administrar el Agente de red ni el Servidor de administración. Tampoco se podrá acceder a la ventana de propiedades del Servidor de administración secundario.
- El asistente de inicio rápido no estará disponible.
- No será posible modificar los ajustes de almacenamiento y notificación relativos a los eventos del Agente de red y del Servidor de administración.
- La sección **Versiones actuales de las aplicaciones** no estará 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 ícono de Configuración ( ) ubicado junto al nombre del Servidor de administración principal.
2. En la página que se abre, vaya a la pestaña **Servidores de administración**.
3. Busque el grupo de administración al que pertenezca el servidor de administración secundario que desee eliminar y seleccione ese servidor.
4. En la línea del menú, haga clic en **Eliminar**.
5. En la ventana que se abre, haga clic en **Aceptar** para confirmar que desea eliminar el Servidor de administración secundario.

El Servidor de administración que supo actuar como principal y el Servidor de administración que supo actuar como secundario se vuelven independientes. La jerarquía deja de existir.

Configuración de la interfaz

Puede configurar la interfaz de Kaspersky Security Center Cloud Console para mostrar u ocultar distintas secciones y elementos de la interfaz según las funciones que utilice.

Para configurar la interfaz de Kaspersky Security Center Cloud Console y adaptarla a las características que utilice:

1. En el menú principal, vaya a la configuración de su cuenta y, a continuación, seleccione **Opciones de interfaz.**
2. En la ventana **Opciones de interfaz** que se abre, habilite o deshabilite las siguientes opciones:
   - **Mostrar protección y cifrado de datos**

     Utilice esta opción para mostrar u ocultar la sección **Operaciones → Protección y cifrado de datos** en la interfaz. Kaspersky Security Center Cloud Console guardará el valor que le asigne a esta opción únicamente para su cuenta de usuario; los demás usuarios podrán definir un valor diferente.

   - **Mostrar funciones de MDR**

     Utilice esta opción para mostrar u ocultar la sección **Supervisión e informes → Incidentes** en la interfaz. Kaspersky Security Center Cloud Console guardará el valor que le asigne a esta opción únicamente para su cuenta de usuario; los demás usuarios podrán definir un valor diferente.

3. Defina el número de dispositivos que Kaspersky Security Center Cloud Console mostrará en los resultados de distribución de las directivas.
4. Haga clic en **Guardar**.

La configuración de la consola queda adaptada a 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 icono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.
2. En la página que se abre, vaya a la pestaña **Servidores de administración**.
3. Seleccione el grupo de administración al que quiere agregar el Servidor de administración virtual.
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 icono de configuración ( ) ubicado junto al nombre del Servidor de administración pertinente.
2. En la página que se abre, vaya a la pestaña **Servidores de administración**.
3. Seleccione el Servidor de administración virtual que desee habilitar o deshabilitar.
4. En la línea del menú, haga clic en el botón **Habilitar/deshabilitar el Servidor de administración virtual**.

Dependiendo del estado que tuviera antes de esta acción, el Servidor de administración virtual cambiará de estado a habilitado o deshabilitado. El nuevo estado aparecerá junto al nombre del Servidor de administración.

Asignar un administrador para un Servidor de administración virtual

Cuando utiliza Servidores de administración virtuales en su organización, es posible que desee asignar un administrador dedicado para cada Servidor de administración virtual. Esto puede ser útil, por ejemplo, cuando una organización crea servidores virtuales para administrar oficinas o departamentos separados o cuando un proveedor de servicios administrados (MSP) desea administrar sus inquilinos a través de servidores virtuales.

Cuando crea un Servidor de administración virtual, hereda la lista de usuarios y todos los derechos de usuario del Servidor de administración principal. Si un usuario tiene derechos de acceso al Servidor principal, este usuario también tiene derechos de acceso al Servidor virtual. Después de la creación, usted configura los derechos de acceso a los servidores de forma independiente. Si desea asignar un administrador solo para un Servidor de administración virtual, asegúrese de que el administrador no 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 uno o más roles 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 del administrador del servidor virtual recién creada no se incluye en las listas de **Derechos de acceso** de las propiedades de ningún servidor, principal o secundario.
- Tiene el derecho **Modificar ACL de objeto** en el área funcional **Características generales → Permisos de usuario**.

Configurar derechos de acceso manualmente

Para asignar un administrador para un Servidor de administración virtual:

1. En el menú principal, cambie al Servidor de administración virtual pertinente:

   a. Haga clic en el ícono de corchete ( ) a la derecha del nombre del Servidor de administración actual.

   b. Seleccione el Servidor de administración requerido.

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

   Se abre la ventana Propiedades del Servidor de administración.

3. En la pestaña **Derechos de acceso**, haga clic en el botón **Agregar**

   Se abre una lista unificada de usuarios del Servidor de administración principal y el Servidor de administración virtual actual.

4. En la lista de usuarios, seleccione la cuenta del administrador que desea asignar para el Servidor de administración virtual y, a continuación, haga clic en el botón **Aceptar**.

   La aplicación agrega el usuario seleccionado a la lista de usuarios en la pestaña **Derechos de acceso**.

5. Marque la casilla ubicada junto a la cuenta agregada y haga clic en el botón **Derechos de acceso**.

6. Configure los derechos que tendrá el administrador sobre el Servidor de administración virtual.

   Para una autenticación correcta, el administrador debe tener, por lo menos, los siguientes derechos:

   - Derecho de **Leer** en el área funcional **Características generales → Funcionalidad básica**
   - Derecho de **Leer** en el área funcional **Características generales → Servidores de administración virtuales**

La aplicación guarda los derechos de usuario modificados en la cuenta de administrador.

Configurar derechos de acceso mediante la asignación de roles de usuario

Como alternativa, puede otorgar los derechos de acceso a un administrador del Servidor de administración virtual a través de roles de usuario. Por ejemplo, esto podría ser útil si desea asignar varios administradores en el mismo Servidor de administración virtual. Si este es el caso, puede asignar a las cuentas de los administradores la misma o más roles de usuario en lugar de configurar los mismos derechos de usuario para varios administradores.

Para asignar un administrador para un Servidor de administración virtual mediante la asignación de roles de usuario:

1. En el Servidor de administración principal, cree un nuevo rol de usuario y, a continuación, especifique todos los derechos de acceso necesarios que un administrador debe tener en el Servidor de administración virtual. Puede crear varios roles, por ejemplo, si desea separar el acceso a diferentes áreas funcionales.

2. En el menú principal, cambie al Servidor de administración virtual pertinente:

   a. Haga clic en el ícono de corchete ( ) a la derecha del nombre del Servidor de administración actual.

   b. Seleccione el Servidor de administración requerido.

3. Asigne el nuevo rol o varios roles a la cuenta de administrador.

Al asignar roles a un usuario, en el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y, luego, seleccione la pestaña **Usuarios**. Si selecciona la pestaña **Grupos** y, luego, asigna roles al grupo en el que el usuario es miembro, el usuario no podrá iniciar sesión en Kaspersky Security Center Cloud Console.

La aplicación asigna el nuevo rol 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 volver a administrar esos dispositivos con Kaspersky Security Center Cloud Console, deberá realizar un sondeo de red y mover los dispositivos del grupo "Dispositivos no asignados" a los grupos de administración que considere pertinentes.

Para eliminar un Servidor de administración virtual:

1. En el menú principal, haga clic en el icono de configuración ( ) ubicado junto al nombre del Servidor de administración.
2. En la página que se abre, vaya a la pestaña **Servidores de administración**.
3. Seleccione el Servidor de administración virtual que desee eliminar.
4. En la línea del menú, haga clic en el botón **Eliminar**.

Se elimina el Servidor de administración virtual.

Supervisión e informes

En esta sección, se describen las prestaciones de supervisión y de generación de informes disponibles en 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.

Una vez que termine con el despliegue de Kaspersky Security Center Cloud Console o cuando ya esté utilizando la solución, podrá configurar las funciones de supervisión e informes para adaptarlas a sus necesidades.

Procedimiento: Supervisión y generación de informes

En esta sección, se describe un escenario para configurar la característica de supervisión y generación de informes de Kaspersky Security Center Cloud Console.

Requisitos previos

Tras completar el despliegue de Kaspersky Security Center Cloud Console en la red de su organización, puede comenzar a supervisar lo que ocurre en la red y a generar informes sobre su funcionamiento.

Etapas

El proceso para configurar la supervisión y la generación de informes en la red de una organización se divide en etapas:

1. **Configurar cambios de estado para los dispositivos**

   Familiarícese con los ajustes que permiten cambiar el estado de los dispositivos en respuesta a distintas condiciones. Al cambiar estas configuraciones, puede cambiar la cantidad de eventos con niveles de importancia Crítica o Advertencia. Cuando configure los cambios de estados para los dispositivos, preste especial atención a lo siguiente:

   - La nueva configuración no debe contravenir las políticas de seguridad de datos de su organización.
   - Cuando se registre un evento de seguridad importante en la red de su organización, podrá brindar una respuesta en un tiempo prudencial.

2. **Configurar las notificaciones sobre los eventos que suceden en los dispositivos cliente**

   Instrucciones: Configurar el envío de notificaciones (por correo electrónico) sobre los eventos de los dispositivos cliente

3. **Cambiar el modo en que la red de seguridad responde al evento Brote de virus**

   Puede modificar los umbrales pertinentes 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:

   - Revisar el widget **Estado de protección**
   - Generar y revisar el **Informe del estado de la protección**

- Generar y revisar 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 protección** y **Estadísticas de amenazas**
   - Inicie y revise la selección de eventos **Crítico**

7. **Controlar la información de las licencias**

   Instrucciones:

   - Agregar el widget **Uso de clave de licencia** al panel y revisarlo
   - Generar y revisar el **Informe de uso de claves de licencia**

Resultados

Al concluir este escenario, podrá mantenerse al corriente de la protección de su red y estará en condiciones de planificar medidas de protección adicionales.

Acerca de los tipos de funciones de supervisión y generación de informes

Los eventos de seguridad que suceden en la red de su organización quedan registrados en la base de datos del Servidor de administración. Kaspersky Security Center Cloud Console utiliza estos eventos para ofrecerle las siguientes funciones de supervisión y generación de informes para su red:

- 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**, **Errores funcionales**, **Advertencias** y **Eventos informativos**
- Por fecha: **Eventos recientes**
- Por tipo: **Solicitudes de usuario** y **Eventos de auditoría**

Puede usar los ajustes disponibles en la interfaz de Kaspersky Security Center Cloud Console para ver y crear selecciones de eventos definidas por el usuario.

Panel y widgets

En esta sección, se brinda información sobre el panel y sobre los widgets que el panel ofrece. Aquí encontrará instrucciones para administrar los widgets y configurar los ajustes de los widgets.

Uso del panel

El panel brinda información gráfica que ayuda a controlar las tendencias de seguridad que se presentan en la red de la organización.

Para acceder al panel de Kaspersky Security Center Cloud Console, ingrese a la sección **Supervisión e informes** y haga 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 protección**
- **Despliegue**
- **Actualización**
- **Estadísticas de amenazas**
- **Otros**

Algunos widgets tienen información de texto con vínculos. Puede hacer clic en esos vínculos para acceder a información detallada.

Al configurar el panel, puede agregar los widgets que le resulten necesarios, ocultar los widgets que no precise, cambiar el tamaño o el aspecto de los widgets, mover los widgets y cambiar la configuración de los widgets.

Agregar widgets al panel

Para agregar widgets al panel:

1. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
2. Haga clic en el botón **Agregar o restaurar widget web**.
3. En la lista de widgets disponibles, seleccione los widgets que desee agregar al panel.

   Los widgets se agrupan por categoría. Para ver los widgets que forman parte de una categoría, haga clic en el corchete angular (>) ubicado junto al nombre de la categoría en cuestión.
4. Haga clic en el botón **Agregar**.

Los widgets seleccionados se agregan al final del panel.

Si lo desea, puede modificar el aspecto y la configuración de los widgets agregados.

Ocultar un widget del panel

Para ocultar uno de los widgets que se muestran en el panel:

1. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee ocultar.
3. Seleccione **Ocultar widget web**.
4. En la ventana **Advertencia** que se abre, haga clic en **Aceptar**.

Se oculta el widget seleccionado. Más tarde, podrá agregar el widget al panel nuevamente.

Mover un widget en el panel

Para mover un widget en el panel:

1. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee mover.

3. Seleccione **Mover**.

4. Haga clic en la ubicación a la que desee mover el widget. Solo puede seleccionar una ubicación que se encuentre ocupada por otro widget.

Los widgets cambiarán de ubicación recíprocamente.

Cambiar el aspecto o el tamaño de un widget

Puede modificar el aspecto de los widgets que contienen un gráfico y hacer que muestren un gráfico de barras o un gráfico de líneas. Algunos widgets también están disponibles en distintos tamaños (compacto, medio y máximo) y pueden redimensionarse.

Para cambiar el aspecto de un widget:

1. En el menú principal, vaya a **Supervisión e informes → Panel**.

2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee modificar.

3. Realice una de las siguientes acciones:

   - Para que el widget se muestre como gráfico de barras, seleccione **Tipo de gráfico: barras**.
   - Para que el widget se muestre como gráfico de líneas, seleccione **Tipo de gráfico: líneas**.
   - Para cambiar el área ocupada por el widget, seleccione uno de los siguientes valores:
     - **Compacto**
     - **Compacto (solo barra)**
     - **Medio (gráfico de anillos)**
     - **Medio (diagrama de barras)**
     - **Máximo**

El widget seleccionado toma el nuevo aspecto.

Cambiar la configuración de un widget

Para modificar la configuración de un widget:

1. En el menú principal, vaya a **Supervisión e informes → Panel**.

2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee cambiar.

3. Seleccione **Mostrar configuración**.

4. En la ventana de configuración del widget, haga los cambios que desee en los ajustes del widget.

5. Haga clic en **Guardar** para guardar los cambios.

Se modifican los ajustes del widget seleccionado.

El conjunto de ajustes disponibles varía según el widget. Estos son algunos de los ajustes comunes:

- **Alcance del widget web** (conjunto de objetos de los que muestra la información el widget): por ejemplo, un grupo de administración o selección de dispositivos.
- **Elija una tarea**: tarea a la que corresponde la información mostrada por el widget.
- **Intervalo de tiempo** (el intervalo de tiempo durante el cual se muestra la información en el widget): entre las dos fechas especificadas; desde la fecha especificada hasta el día actual; o desde el día actual menos el número especificado de días hasta el día actual.
- **Fijar en Crítico si esto se cumple** y **Fijar en Advertencia si esto se cumple**: las reglas que determinan el color de un semáforo.

Después de cambiar la configuración del widget, puede actualizar los datos en el widget manualmente.

Para actualizar datos en un widget:

1. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
2. Haga clic en el ícono de configuración (⚙) ubicado junto al widget que desee mover.
3. Seleccione **Actualizar**.

Se actualizan los datos del widget.

Acerca del modo solo panel

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

Un usuario para el que se habilitado el modo solo panel está sujeto a las siguientes restricciones:

- El usuario no tiene acceso al menú principal, lo cual le impide modificar los ajustes de protección de la red.
- El usuario no puede realizar ninguna acción con los widgets: no puede, por ejemplo, agregar widgets nuevos ni quitar los widgets agregados. Debido a estas restricciones, usted deberá agregar al panel todos los widgets que el usuario precise y deberá encargarse, asimismo, de configurarlos (tendrá que fijar la regla de conteo de objetos, definir el intervalo de tiempo, etc.).

Un usuario no puede asignarse a sí mismo el modo solo panel. Si desea trabajar en este modo, comuníquese con su administrador de sistemas, con su proveedor de servicios administrados (MSP) o con un usuario que tenga el derecho **Modificar ACL de objetos** en el área funcional **Características generales: Permisos de usuario**.

Configuración del modo solo panel

Si desea configurar el modo solo panel, asegúrese primero de que se cumplan los siguientes requisitos:

- Usted cuenta con el derecho **Modificar ACL de objetos** en el área funcional **Características generales: Permisos de usuario**. Si no tiene este derecho, no encontrará la pestaña para configurar el modo.
- El usuario tiene asignado el derecho Leer en el área funcional **Características generales**: **Funcionalidad básica**.

Si creó una jerarquía de Servidores de administración en su red, para configurar el modo solo panel, vaya al Servidor que tenga disponible la cuenta de usuario en la pestaña **Usuarios** de la sección **Usuarios y roles** → **Usuarios y grupos**. El servidor puede ser un servidor principal o un servidor secundario físico. Este modo no puede ajustarse en servidores virtuales.

Para configurar el modo solo panel:

1. En el menú principal, vaya a **Usuarios y roles** → **Usuarios y grupos** y luego seleccione la pestaña **Usuarios**.
2. Haga clic en el nombre de la cuenta de usuario para la que desee ajustar el panel con widgets.
3. En la ventana que se abre, que contendrá los ajustes de la cuenta, seleccione la pestaña **Panel**.

   En la pestaña que se abre, verá un panel. El panel será el mismo panel para usted que para el usuario.
4. Si la opción **Mostrar la consola en modo solo panel** está habilitada, cambie la posición del interruptor para deshabilitarla.

   El sistema no le permitirá hacer cambios en el panel mientras esta opción se encuentre habilitada. Una vez que deshabilite esta opción, podrá operar con los widgets.
5. Configure la apariencia del panel. El conjunto de widgets preparados en la pestaña **Panel** estará disponible para el usuario con la cuenta personalizable. El usuario no podrá agregar widgets nuevos al panel ni podrá quitar los widgets agregados; tampoco podrá modificar los ajustes o el tamaño de estos elementos. Debido a estas limitaciones, debe ocuparse usted de ajustar los widgets de manera tal que el usuario tenga acceso a las estadísticas sobre la protección de la red. A tal fin, la pestaña **Panel** le permitirá operar con los widgets tal como si estuviera en la sección **Supervisión e informes** → **Panel**. Podrá hacer lo siguiente:
   - Agregar nuevos widgets al panel.
   - Ocultar widgets que el usuario no necesite.
   - Mover los widgets y colocarlos en otro orden.
   - Cambiar el tamaño o el aspecto de los widgets.
   - Modificar los ajustes de los widgets.
6. Active el interruptor para habilitar la opción **Mostrar la consola en modo solo panel**.

   Una vez que habilite esta opción, el usuario solamente tendrá acceso al panel. Podrá ver las estadísticas, pero no podrá hacer cambios en los ajustes de protección de la red ni podrá modificar el aspecto del panel. Como el panel es el mismo para usted que para el usuario, usted tampoco podrá hacer ajustes en el panel.

Si deja esta opción deshabilitada, el usuario tendrá acceso al menú principal y, desde allí, podrá realizar distintas acciones en Kaspersky Security Center Cloud Console, como modificar los widgets y cambiar los ajustes de seguridad.

7. Haga clic en el botón **Guardar** cuando haya terminado de configurar el modo solo panel. El usuario no verá el panel preparado sino hasta que usted guarde los cambios.

8. Si el usuario desea ver las estadísticas de las aplicaciones de Kaspersky compatibles y necesita, para ello, contar con determinados derechos de acceso, configure los derechos del usuario. Tras ello, el usuario verá los datos de las aplicaciones de Kaspersky en los widgets correspondientes a esas aplicaciones.

Al concluir este procedimiento, el usuario podrá iniciar sesión en Kaspersky Security Center Cloud Console con su cuenta personalizada y utilizar el modo solo panel para monitorear las estadísticas sobre la protección de la red.

Informes

En esta sección, se brindan instrucciones para trabajar con los informes, administrar plantillas de informes personalizadas, usar plantillas de informes para generar nuevos informes y crear tareas de entrega de informes.

Utilización de informes

La función Informes permite obtener información numérica detallada sobre la seguridad de la red de la organización. La información puede guardarse en un archivo, imprimirse o enviarse por correo electrónico.

Para acceder a los informes de Kaspersky Security Center Cloud Console, ingrese a la sección **Supervisión e informes** y haga clic en **Informes**.

Por defecto, los informes contienen información de los últimos treinta días.

Kaspersky Security Center Cloud Console tiene un conjunto de informes predeterminado para las siguientes categorías:

- **Estado de protección**
- **Despliegue**
- **Actualización**
- **Estadísticas de amenazas**
- **Otros**

Puede crear plantillas de informe personalizadas y modificar o eliminar las plantillas de informe existentes.

Puede crear informes basados en las plantillas existentes, exportar informes a archivos y crear tareas de entrega de informes.

Crear una plantilla de informe

Para crear una plantilla de informe:

1. En el menú principal, vaya a **Supervisión e informes → Informes**.
2. Haga clic en **Agregar**.

   Se abre el Asistente de nueva plantilla de informe. Avance por el asistente utilizando el botón **Siguiente**.
3. Ingrese el nombre del informe y seleccione el tipo de informe.
4. En el paso **Alcance** del asistente, seleccione el conjunto de dispositivos cliente (grupo de administración, selección de dispositivos, dispositivos seleccionados o todos los dispositivos de red) cuyos datos se mostrarán en informes que se basen en esta plantilla de informe.
5. En el paso **Período del informe**, especifique el período del informe. Los valores disponibles son los siguientes:

   - Entre dos fechas específicas
   - Desde una fecha específica hasta la fecha de creación del informe
   - Desde cierta cantidad de días antes de la creación del informe hasta la fecha de creación del informe

   Esta página puede no aparecer para algunos informes.
6. Haga clic en **Aceptar** para cerrar el asistente.
7. Realice una de las siguientes acciones:

   - Haga clic en el botón **Guardar y ejecutar** para guardar la nueva plantilla de informe y crear un informe basado en ella.

     Se guardará la plantilla de informe. Se generará el informe.
   - Haga clic en el botón **Guardar** para guardar la nueva plantilla de informe.

     Se guardará la plantilla de informe.

Puede utilizar la nueva plantilla para generar y ver informes.

Ver y editar las propiedades de una plantilla de informe

Puede ver y editar las propiedades básicas de las plantillas de informe (por ejemplo, el nombre de las plantillas o los campos que se muestran en los informes).

Para ver y editar las propiedades de una plantilla de informe:

1. En el menú principal, vaya a **Supervisión e informes → Informes**.
2. Marque la casilla ubicada junto a la plantilla de informe cuyas propiedades desee ver o editar.

   Como alternativa, genere un informe y luego haga clic en el botón **Editar**.
3. Haga clic en el botón **Abrir las propiedades de la plantilla del informe**.

   Se abre la ventana **Editando informe "<nombre del informe>"**. La pestaña **General** estará seleccionada.
4. Modifique las propiedades de la plantilla de informe:

   - Pestaña **General**:

- Nombre de la plantilla de informe
- **Cantidad máxima de entradas para mostrar**

  Si esta opción está habilitada, la tabla con los datos detallados del informe mostrará, como máximo, el número de entradas indicado aquí. Tenga en cuenta que esta opción no afecta el número máximo de eventos que se pueden incluir en el informe si se lo exporta un archivo.

  Las entradas del informe se ordenan primero siguiendo las reglas especificadas en la sección **Campos → Campos Detalles** de las propiedades de la plantilla de informe, y luego se conservan solo las primeras de las entradas resultantes. El encabezado de la tabla con los datos detallados del informe indica el número de entradas mostradas y el total de entradas disponibles que coinciden con otros parámetros de la plantilla del informe.

  Si deshabilita esta opción, se mostrarán todas las entradas disponibles en la tabla con los datos detallados del informe. No recomendamos deshabilitar esta opción. Al limitar el número de entradas que se muestran en un informe, se aminora la carga en el sistema de administración de bases de datos y se reduce el tiempo requerido para generar y exportar el informe. Algunos de los informes contienen demasiadas entradas. En tales casos, no es sencillo leer y analizar todas las entradas. Además, cuando se genera un informe de este tipo, se corre el riesgo de que el dispositivo se quede sin memoria; de ocurrir este problema, no será posible siquiera ver el informe.

  Esta opción está activada de forma predeterminada. El valor predeterminado es 1000.

  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 de 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 activada de forma predeterminada.

- **Hasta el nivel de anidamiento**

El informe incluirá datos de los servidores de administración secundarios y virtuales que se encuentren <n> o más niveles de anidamiento por debajo del Servidor de administración con el que se esté trabajando, siendo <n> el valor especificado.

El valor predeterminado es 1. Puede cambiar este valor si necesita recuperar información de servidores de administración secundarios que se encuentren aún más abajo en el árbol.

- Intervalo de espera de datos (min)

  Antes de generar el informe, el Servidor de administración para el que se haya creado la plantilla de informe esperará, durante el tiempo especificado, a que los servidores de administración secundarios le envíen datos. Transcurrido este período de espera, el Servidor generará el informe aunque no haya recibido información de los servidores de administración secundarios. En ese caso, en lugar de los datos reales, el informe mostrará el valor **N/D** (no disponible) o, si la opción **Almacenar en caché los datos de los Servidores de administración secundarios** está habilitada, mostrará información tomada de la caché.

  El valor predeterminado es 5 (minutos).

- Almacenar en caché los datos de los Servidores de administración secundarios

  Los servidores de administración secundarios transfieren datos periódicamente al Servidor de administración para el que se ha creado la plantilla de informe. Una vez allí, los datos transferidos se guardan en una caché.

  Si, al momento de generar un informe, el Servidor de administración no puede recibir datos de algún Servidor de administración secundario, el informe contendrá los datos de esta caché. La fecha en que los datos se transfirieron a la caché estará indicada en el informe.

  Si habilita esta opción, podrá ver datos de los servidores de administración secundarios incluso cuando no se pueda obtener información actualizada. Sin embargo, los datos mostrados podrían ser obsoletos.

  Esta opción está deshabilitada de forma predeterminada.

- Frecuencia de actualización de la caché (h)

  Los servidores de administración secundarios transfieren datos a intervalos regulares al Servidor de administración para el que se ha creado la plantilla de informe. Puede especificar el largo de este intervalo en horas. Si fija el valor en 0 horas, solamente se transferirá información cuando se genere el informe.

  El valor predeterminado es 0.

- Transferir información detallada desde los Servidores de administración secundarios

  En el informe generado, la tabla con los datos detallados del informe contendrá datos de los servidores de administración secundarios que estén subordinados al Servidor de administración para el cual se haya creado la plantilla de informe.

  Si habilita esta opción, los informes tardarán más tiempo en generarse y habrá más tráfico entre los servidores de administración. Sin embargo, podrá ver toda la información en un solo informe.

  En lugar de habilitar esta opción, podría analizar los datos detallados de un informe para detectar un Servidor de administración secundario con problemas y, hecho esto, generar ese mismo informe únicamente para ese Servidor de administración.

  Esta opción está deshabilitada de forma predeterminada.

- Pestaña **Campos**

  Seleccione los campos que se mostrarán en el informe y ordénelos con los botones **Subir** y **Bajar**. Use los botones **Agregar** o **Editar** para especificar si los campos se usarán para filtrar y ordenar los datos del informe.

  La sección **Filtros de los campos Detalles** contiene un botón llamado **Convertir filtros**. Haga clic en este botón para comenzar a usar el formato de filtrado ampliado. Este formato permite combinar, mediante la operación lógica OR, las condiciones de filtrado especificadas en distintos campos. Si hace clic en el botón, se abrirá el panel **Convertir filtros** en el lado derecho. Haga clic en el botón **Convertir filtros** para confirmar la conversión. Tras ello, podrá definir un filtro convertido con condiciones de la sección **Campos Detalles** que se apliquen utilizando la operación lógica OR.

  > Cuando un informe se convierte al formato que permite definir condiciones de filtrado complejas, el mismo deja de ser compatible con las versiones anteriores de Kaspersky Security Center (11 y anteriores). Los informes convertidos no incluyen datos de servidores de administración secundarios basados en versiones incompatibles.

5. Haga clic en **Guardar** para guardar los cambios.

6. Cierra la ventana **Editando informe "<nombre del informe>"**.

La plantilla de informe actualizada aparece en la lista de plantillas de informe.

Exportación de un informe a un archivo

Puede guardar uno o varios informes en los formatos XML, HTML y PDF. Kaspersky Security Center Cloud Console permite exportar hasta diez informes por vez a archivos de estos formatos.

Para exportar un informe a un archivo:

1. En el menú principal, vaya a **Supervisión e informes** → **Informes**.

2. Elija los informes que desee exportar.

   Si selecciona más de 10 informes, el botón **Exportar informe** se deshabilitará.

3. Haga clic en el botón **Exportar informe**.

4. En la ventana que se abrirá, defina los siguientes parámetros de exportación:

   - **Nombre de archivo**.

     Si seleccionó un único informe para exportar, ingrese el nombre que desee dar al archivo del informe.

     Si seleccionó más de un informe, el nombre de cada archivo será el de la plantilla con la que se haya generado el informe seleccionado.

   - **Número máximo de entradas**.

     Especifique el número máximo de entradas incluidas en el archivo del informe. El valor predeterminado es 10000.

   - **Formato de archivo**.

     Seleccione el formato de archivo al que se exportará el informe: XML, HTML o PDF. Si exporta más de un informe, cada informe seleccionado se guardará en un archivo individual del formato seleccionado.

5. Haga clic en el botón **Exportar informe**.

El informe se guarda en un archivo del formato seleccionado.

Generar y ver un informe

Para crear y ver un informe:

1. En el menú principal, vaya a **Supervisión e informes → Informes**.
2. Haga clic en el nombre de la plantilla de informe con la que desee crear el informe.

   Se creará y mostrará un informe basado en la plantilla seleccionada.

> Los datos de los informes se muestran únicamente en inglés; no están disponibles en otros idiomas de localización.

El informe contendrá los siguientes datos:

- En la pestaña **Resumen**:
  - El nombre del informe, el tipo de informe, una descripción breve, el período comprendido por el informe e información sobre el grupo de dispositivos para los que se generó el informe.
  - Un gráfico con los datos más representativos del informe.
  - Una tabla unificada con los indicadores calculados del informe.
- En la pestaña **Detalles**, una tabla con datos detallados del informe.

Crear una tarea de entrega de informes

Puede crear una tarea para entregar informes específicos.

Para crear una tarea de entrega de informes:

1. En el menú principal, vaya a **Supervisión e informes → Informes**.
2. Active las casillas ubicadas junto a las plantillas de informe para las que desee crear una tarea de entrega de informes.
3. Haga clic en el botón **Crear tarea de entrega**.

   Se inicia el Asistente para crear nueva tarea. Utilice el botón **Siguiente** para avanzar a un nuevo paso del asistente.
4. En el paso **Configuración de tarea nueva** del asistente, ingrese el nombre de la tarea.

   El nombre predeterminado es **Entregar informes**. Si ya existe una tarea con este nombre, se agrega un número de secuencia (<N>) al nombre de la tarea.

5. En el paso **Configuración del informe** del asistente, especifique la siguiente configuración:

   a. Seleccione las plantillas de informe que entregará la tarea.

   b. Defina el formato de los informes: HTML, XLS o PDF.

      Se requiere la herramienta wkhtmltopdf para convertir un informe a PDF. Cuando selecciona la opción PDF, el Servidor de administración verifica si la herramienta wkhtmltopdf está instalada en el dispositivo. Si la herramienta no está instalada, la aplicación muestra un mensaje sobre la necesidad de instalar la herramienta en el dispositivo del Servidor de administración. Instale la herramienta manualmente y luego continúe con el siguiente paso.

   c. Indique si los informes se enviarán por correo electrónico y, de ser así, defina los ajustes de notificación por correo electrónico.

      Puede especificar hasta 20 direcciones de correo electrónico. Para separar direcciones de correo electrónico, presione **Intro**. También puede pegar una lista de direcciones de correo electrónico separadas por comas y luego presionar **Intro**.

6. En el paso **Configurar programación de tarea** del asistente, seleccione la programación de inicio de la tarea.

   Están disponibles las siguientes opciones de programación de tareas:

   - Manual

     La tarea no se ejecutará automáticamente. Solo se la podrá iniciar en forma manual.

     Esta opción está seleccionada de forma predeterminada.

   - Cada N minutos

     La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la hora indicada en el día en que se cree la tarea. Cada ejecución estará separada de la anterior por el número de minutos que indique.

     De forma predeterminada, la tarea se ejecutará cada treinta minutos, a partir de la hora actual del sistema.

   - Cada N horas

     La tarea se ejecutará periódicamente, a intervalos regulares, a partir de la fecha y hora indicadas. Cada ejecución estará separada de la anterior por el número de horas que indique.

     De manera predeterminada, la tarea se ejecutará cada 6 horas, a partir de la fecha y hora actuales del sistema.

   - Cada N días

     La tarea se ejecutará periódicamente, a intervalos regulares. Cada ejecución estará separada de la anterior por el número de días indicado. Esta opción permite elegir la fecha y hora de la primera ejecución. Podrá configurar estos dos ajustes si son compatibles con la aplicación para la que esté creando la tarea.

     De forma predeterminada, la tarea se ejecutará todos los días, a partir de la fecha y hora actuales del sistema.

   - Cada N semanas

La tarea se ejecutará periódicamente, a intervalos regulares, en el día de la semana y a la hora que especifique. Cada ejecución estará separada de la anterior por el número de semanas que indique.

Por defecto, la tarea se ejecutará cada lunes a la hora actual del sistema.

- **Mensual**

  La tarea se ejecutará periódicamente, en el día del mes y a la hora que indique.

  Si el día elegido no forma parte de un mes, la tarea se ejecutará el último día de ese mes.

  Por defecto, la tarea se ejecutará el primer día de cada mes, a la hora actual del sistema.

- **En los días especificados**

  La tarea se ejecutará periódicamente, en los días del mes y a la hora que indique.

  De manera predeterminada, no se selecciona ningún día del mes. La hora de inicio predeterminada es a las 18:00.

- **Ante brotes de virus**

  La tarea se ejecutará cuando ocurra un evento *Brote de virus*. Seleccione los tipos de aplicaciones que se usarán para controlar si ocurre un brote de virus. Están disponibles los siguientes tipos de aplicaciones:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para defensa del perímetro
  - Antivirus para sistemas de correo

  Por defecto, están seleccionados todos los tipos de aplicaciones.

  En algunos casos, querrá ejecutar tareas diferentes según el tipo de aplicación de seguridad que dé aviso de un brote de virus. De ser así, anule la selección de los tipos de aplicaciones que no necesite.

- **Al completarse otra tarea**

  La tarea actual se iniciará después de que se complete otra tarea. 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 el dispositivo** y hacer que, una vez completada esa tarea, se ejecute la tarea *Análisis antivirus* como una tarea desencadenante.

  Debe seleccionar la tarea desencadenante de la tabla y el estado con el que esta tarea debe completarse (**Completada correctamente** o **Error**).

  Si es necesario, puede buscar, ordenar y filtrar las tareas en la tabla de la siguiente manera:

  - Ingrese el nombre de la tarea en el campo de búsqueda para buscar la tarea por su nombre.
  - Haga clic en el ícono de ordenar para ordenar las tareas por nombre.

    De manera predeterminada, las tareas se clasifican en orden alfabético ascendente.
  - Haga clic en el ícono de filtro y, en la ventana que se abre, filtre las tareas por grupo y luego haga clic en el botón **Aplicar**.

7. En este paso del asistente, configure otras opciones de programación de tareas:

- En la sección **Programación de la tarea**, verifique o reconfigure la programación previamente seleccionada, y establezca el intervalo de tiempo, los días del mes o la semana, establezca la condición de brote de virus o la finalización de otra tarea como disparador para iniciar la tarea. También se puede especificar una hora de inicio en esta sección si se selecciona una programación aplicable.

- En la sección **Configuración adicional**, especifique las siguientes configuraciones:

  - **Ejecutar tareas no realizadas**

    Esta opción determina el comportamiento de la tarea cuando la misma está por iniciarse y uno de los dispositivos cliente no está visible en la red.

    Si esta opción está habilitada, el sistema intentará iniciar la tarea la siguiente vez que la aplicación de Kaspersky se ejecute en el dispositivo cliente. Si la programación de la tarea es **Manual**, **Una vez** o **Inmediatamente**, la tarea se iniciará inmediatamente después de que el dispositivo aparezca en la red o inmediatamente después de que el dispositivo sea incluido en el alcance de la tarea.

    Si esta opción está deshabilitada, solo las tareas programadas se ejecutan en los dispositivos cliente. Para la programación **Manual**, **Una vez** e **Inmediatamente**, las tareas se ejecutan solo en los dispositivos cliente que están visibles en la red. Podría deshabilitar esta opción para, por ejemplo, una tarea que consuma muchos recursos y que solo deba ejecutarse fuera del horario laboral.

    Esta opción está deshabilitada de forma predeterminada.

  - **Utilizar retardo aleatorio automático para el inicio de la tarea**

    Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo que especifique. Se realizará, de este modo, un *inicio distribuido*. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

    La hora de inicio distribuida se calcula automáticamente cuando se crea una tarea. El cálculo tiene en cuenta el número de dispositivos cliente a los que la tarea está asignada. Las ejecuciones posteriores a la inicial ocurren siempre a la hora de inicio calculada. Sin embargo, tenga en cuenta que si modifica la configuración de la tarea o inicia la tarea manualmente, la hora de inicio calculada cambiará.

    Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

  - **Utilizar el retardo aleatorio automático para el inicio de la tarea dentro de un intervalo de**

    Si esta opción está habilitada, la tarea se iniciará en los dispositivos cliente en un punto aleatorio del intervalo de tiempo especificado. El inicio distribuido evita que, al ejecutarse una tarea programada, el Servidor de administración reciba simultáneamente un gran número de solicitudes de los dispositivos cliente.

    Si esta opción está deshabilitada, la tarea se iniciará en los dispositivos cliente siguiendo la programación definida.

    Esta opción está deshabilitada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

  - **Detener la tarea si tarda más de**

Una vez que transcurra el período especificado, la tarea se detendrá automáticamente, se haya completado o no.

Habilite esta opción si desea que las tareas que tarden mucho en completarse se interrumpan o se detengan.

Esta opción está deshabilitada de forma predeterminada. El tiempo de ejecución por defecto para las tareas es de 120 minutos.

8. En el paso **Seleccione una cuenta con la que ejecutar la tarea** del asistente, especifique las credenciales de la cuenta de usuario que se utiliza para ejecutar la tarea.

9. Si desea modificar otras configuraciones de la tarea después de crearla, en el paso **Finalizar la creación de la tarea** del asistente, habilite la opción **Abrir los detalles de la tarea cuando se complete la creación** (esta opción está habilitada de manera predeterminada).

10. Haga clic en el botón **Finalizar** para crear la tarea y cerrar el asistente.

    Se creará la tarea de entrega de informes. Si la opción **Abrir los detalles de la tarea cuando se complete la creación** está habilitada, se abrirá la ventana de configuración de la tarea.

Eliminación de plantillas de informes

Para eliminar una o varias plantillas de informes:

1. En el menú principal, vaya a **Supervisión e informes → Informes**.

2. Marque las casillas ubicadas junto a las plantillas de informes que desee eliminar.

3. Haga clic en el botón **Eliminar**.

4. En la ventana que se abre, haga clic en **Aceptar** para confirmar su selección.

Se eliminan las plantillas de informes seleccionadas. Si las plantillas formaban parte de una o más tareas de entrega de informes, se las eliminará también de esas tareas.

Eventos y selecciones de eventos

En esta sección, se brinda información sobre los eventos y las selecciones de eventos, sobre los tipos de eventos que ocurren en los componentes de Kaspersky Security Center Cloud Console y sobre cómo puede administrar el bloqueo de eventos frecuentes.

Acerca de los eventos de Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console permite recibir información sobre los eventos que ocurren en el Servidor de administración y en las aplicaciones de Kaspersky que se instalan en los dispositivos administrados. La información sobre estos eventos se guarda en la base de datos del Servidor de administración. Puede exportar esta información a un sistema SIEM externo. Al hacerlo, permitirá que los administradores del sistema SIEM respondan oportunamente a los sucesos del sistema de seguridad que se registren en los dispositivos o grupos de dispositivos administrados.

Eventos por tipo

Los eventos disponibles en Kaspersky Security Center Cloud Console son de dos tipos:

- 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** de 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 *error funcional* es un evento que se registra cuando ocurre un problema, fallo o error graves en el funcionamiento de la aplicación o en la ejecución de un procedimiento.
- Una *advertencia* es un evento que no necesariamente es grave, pero que anticipa un posible problema en el futuro. La mayoría de los eventos se catalogan como advertencias si, a pesar de que el evento haya ocurrido, la aplicación puede recuperarse sin sufrir una pérdida de información o de funcionalidad.
- Un evento *informativo* es un evento que se registra para informar que una operación o procedimiento se completaron sin errores o que la aplicación funciona correctamente.

Cada evento tiene asignado un plazo de almacenamiento, período durante el cual se lo puede ver o modificar dentro de 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 eventos. En esta sección, se enumeran los tipos de eventos que pueden ocurrir en el Agente de red y en el Servidor de administración 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**. El texto que se muestra en Kaspersky Security Center Cloud Console cuando se configuran o suceden los eventos.
- **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). Un código que se utiliza al examinar y procesar los eventos mediante las vistas públicas que se ofrecen 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 la licencia	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 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

			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 cree una tarea que se ejecute cuando ocurra el evento.	180 días
El dispositivo ha cambiado a no administrado	4111	KLSRV_HOST_OUT_CONTROL	Este tipo de eventos ocurren si un dispositivo administrado es visible en la red pero no se ha conectado al Servidor de administración durante un período específico. Averigüe qué impide el correcto funcionamiento del Agente de red en el dispositivo. El problema podría deberse a un inconveniente en la red, por ejemplo, o al hecho de que el Agente de red se haya eliminado del dispositivo.	180 días
El estado del dispositivo es Crítico	4113	KLSRV_HOST_STATUS_CRITICAL	Este tipo de evento ocurre cuando se le asigna el estado *Crítico* a un dispositivo administrado. Puede configurar las condiciones bajo las cuales el estado del dispositivo se cambia a *Crítico*.	180 días
Modo de funcionalidad limitada	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Este tipo de evento ocurre cuando Kaspersky Security Center Cloud Console pasa a operar con sus funciones básicas, sin las características Administración de dispositivos móviles y Administración de vulnerabilidades y parches. Las causas de este evento y las maneras de responder son las siguientes: • El periodo de vigencia de la licencia ha caducado. Agregue una licencia que permita usar el modo de funcionalidad completa de Kaspersky Security Center Cloud Console (agregue un código de activación válido o un archivo de clave en el 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 está por caducar	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Este tipo de evento ocurre cuando se acerca la fecha de caducidad de una licencia comercial.	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. El número de días no se puede modificar. Si el Servidor de administración se encuentra apagado el día especificado antes de la fecha de caducidad de la licencia, el evento no se publicará sino hasta el día siguiente. Cuando caduca la licencia comercial, Kaspersky Security Center Cloud Console solo brinda acceso a las funciones básicas. Puede responder al evento de los siguientes modos: • Asegúrese de tener una clave de licencia de reserva agregada 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 caducó	4132	KLSRV_CERTIFICATE_EXPIRED	Este tipo de evento ocurre cuando caduca el certificado del Servidor de administración para Administración de dispositivos móviles. Debe actualizar el certificado caducado.	180 días
Se revocaron las actualizaciones de los módulos de la aplicación de Kaspersky	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Este tipo de evento ocurre cuando los especialistas técnicos de Kaspersky revocan una actualización sin interrupciones (tales actualizaciones tienen el estado *Revocada*) y resulta necesario, por ejemplo, actualizar a una versión más nueva. El evento afecta a los parches de Kaspersky Security Center Cloud Console, no a los módulos de las aplicaciones de Kaspersky administradas. La razón por la que no se instaló la actualización sin interrupciones se indica en el evento.	180 días
Auditoría: la exportación a SIEM produjo un error	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Los eventos de este tipo ocurren cuando la exportación de eventos al sistema SIEM falla debido a un error de conexión con el sistema SIEM.	180 días

Eventos del Servidor de administración: nivel Error funcional

La siguiente tabla muestra los eventos del Servidor de administración de Kaspersky Security Center Cloud Console que tienen el nivel de importancia **error funcional**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Para el Servidor de administración, también puede ver y configurar la lista de eventos en las propiedades del Servidor de administración. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Servidor de administración: nivel Error funcional

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado

Límite de instalaciones excedido en uno de los grupos de aplicaciones con licencia	4126	KLSRV_INVLICPROD_EXCEDED	El Servidor de administración genera eventos de este tipo periódicamente (cada una hora). Este tipo de evento ocurre cuando Kaspersky Security Center Cloud Console se utiliza para administrar claves de licencia de aplicaciones de terceros y se supera el número de instalaciones permitidas por la clave de licencia de la aplicación desarrollada por un tercero. 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, utilice la característica de grupos de aplicaciones con licencia. Un grupo de aplicaciones con licencia está formado por aplicaciones de terceros que cumplen con los criterios que usted define.	180 días
Error al sondear el segmento de la nube	4143	KLSRV_KLCLOUD_SCAN_ERROR	Los eventos de este tipo ocurren cuando el Servidor de administración no puede sondear un segmento de red en un entorno de nube. Lea los detalles en la descripción del evento y responda en consecuencia.	No se almacena

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 la licencia	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 estado inactivo en la red por mucho tiempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Este tipo de evento ocurre cuando un dispositivo administrado se encuentra inactivo durante cierto tiempo. 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 estado inactivo en la red por mucho tiempo** mediante Kaspersky Security Center Cloud Console. • Especifique el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo mediante 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 en las cuales el estado del dispositivo se cambia a *Advertencia*.	90 días
Pronto se alcanzará el límite de instalaciones para uno de los	4127	KLSRV_INVLICPROD_FILLED	Los eventos de este tipo ocurren cuando el número de instalaciones de aplicaciones de terceros incluidas en un grupo de aplicaciones con licencia alcanza el 90 % del	90 días

grupos de aplicaciones con licencia			valor máximo permitido especificado 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, utilice la característica de grupos de aplicaciones con licencia.	
Se solicitó el certificado	4133	KLSRV_CERTIFICATE_REQUESTED	Este tipo de evento ocurre cuando un certificado de la característica Administración de dispositivos móviles no se vuelve a emitir automáticamente. Estas pueden ser las causas del evento y las respuestas adecuadas: • Se intentó reemitir automáticamente un certificado para el que estaba deshabilitada la opción **Se solicitó el certificado**. Esto puede deberse a un error ocurrido durante la creación del certificado. Es posible que se requiera la reemisión manual del certificado. • Si utiliza una integración con una infraestructura de clave pública, la causa podría ser la falta de un atributo SAM-Account-Name de la cuenta utilizada para la integración con PKI y para la emisión del certificado. Revise las propiedades de la cuenta.	90 días
Se eliminó el certificado	4134	KLSRV_CERTIFICATE_REMOVED	Este tipo de evento ocurre cuando un administrador elimina un certificado de cualquier tipo (general, de correo o de VPN) para Administración de dispositivos móviles. 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 caducó	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 caduca, debe 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 pudo	4138	KLSRV_GCM_DEVICE_ERROR	Los eventos de este tipo ocurren cuando la	90 días

enviar el mensaje de FCM al dispositivo móvil			Administración de dispositivos móviles está configurada para usar Google Firebase Cloud Messaging (FCM) para conectarse a dispositivos móviles administrados con un sistema operativo Android y el servidor de FCM no puede manejar algunas de las solicitudes recibidas del Servidor de administración. Lo que esto significa es que algunos de los dispositivos móviles administrados no recibirán una notificación push. 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").	
Error de HTTP al enviar un mensaje del FCM al servidor de FCM	4139	KLSRV_GCM_HTTP_ERROR	Los eventos de este tipo ocurren cuando la Administración de dispositivos móviles está configurada para usar Google Firebase Cloud Messaging (FCM) para conectar dispositivos móviles administrados con el sistema operativo Android y el servidor de FCM devuelve al Servidor de administración una solicitud con un código HTTP distinto de 200 (OK). 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 responda en consecuencia.	90 días
No se pudo enviar el mensaje de FCM al servidor de FCM	4140	KLSRV_GCM_GENERAL_ERROR	Este tipo de evento ocurre cuando suceden errores inesperados del lado del Servidor de administración al utilizar el protocolo HTTP de 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 de SIEM produjo un error	5120	KLAUD_EV_SIEM_TEST_FAILED	Los eventos de este tipo ocurren cuando se produce un error en 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 un límite de licencia.	30 días
Se detectó 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 movió 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
Dispositivo eliminado del grupo: estuvo inactivo en la red por 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

El límite de instalaciones está por alcanzarse (se consumió más del 95 %) en uno de los grupos de aplicaciones con licencia	4128	KLSRV_INVLICPROD_EXPIRED_SOON	Los eventos de este tipo ocurren cuando el número de instalaciones de aplicaciones de terceros incluidas en un grupo de aplicaciones con licencia alcanza el 90 % del valor máximo permitido especificado 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, utilice la característica de grupos de aplicaciones con licencia.	30 días
Se han encontrado archivos para enviar a Kaspersky para su análisis	4131	KLSRV_APS_FILE_APPEARED		30 días
El id. de instancia de FCM ha cambiado en este dispositivo móvil	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	Los eventos de este tipo ocurren cuando el token de Firebase Cloud Messaging (FCM) cambia en el dispositivo. Para obtener información sobre la rotación de tokens de FCM, consulte la documentación del servicio Firebase.	30 días
Las actualizaciones se copiaron 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 en una carpeta específica.	30 días
Se estableció 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: agregar un Servidor de administración secundario.	30 días
Se estableció la conexión con el Servidor de administración principal	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 días
Las bases de datos se han actualizado (En Kaspersky Security Center Cloud Console, este tipo de evento solamente está disponible para servidores de administración secundarios).	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 disponibilidad de KSN se verificó correctamente	7718	KSNPROXY_STARTED_CON_CHK_OK		30 días

El Proxy de KSN se detuvo	7720	KSNPROXY_STOPPED		30 días
Auditoría: Se estableció la conexión con el Servidor de administración	4147	KLAUD_EV_SERVERCONNECT		30 días
Auditoría: El objeto se modificó	4148	KLAUD_EV_OBJECTMODIFY	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 se modificó	4150	KLAUD_EV_TASK_STATE_CHANGED	Este evento ocurre, por ejemplo, cuando una tarea no se completa debido a un error.	30 días
Auditoría: La configuración del grupo se modificó	4149	KLAUD_EV_ADMGROUP_CHANGED	Los eventos de este tipo ocurren cuando se edita un grupo de seguridad.	30 días
Auditoría: Se importaron o exportaron claves de cifrado del Servidor de administración	5100	KLAUD_EV_DPEKEYSEXPORT		30 días
Auditoría: la prueba de conexión al servidor de SIEM se realizó correctamente	5110	KLAUD_EV_SIEM_TEST_SUCCESS		30 días

Eventos del Agente de red

En esta sección, se brinda información sobre los eventos relacionados con el Agente de red.

Eventos del Agente de red: nivel Error funcional

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center que tienen el nivel de gravedad **error funcional**.

Puede definir los ajustes de notificación y los ajustes de almacenamiento para cada uno de los eventos que pueda generar una aplicación; para ello debe dirigirse a la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Agente de red: nivel Error funcional

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Error de	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Este tipo de evento ocurre cuando no se puede	30 días

instalación de la actualización			completar la instalación automática de actualizaciones y parches para los componentes de Kaspersky Security Center Cloud Console. 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	Este tipo de evento ocurre cuando se utilizan las funciones Administración de vulnerabilidades y parches y Administración de dispositivos móviles y ocurre un error al instalar una actualización para el software de un tercero. Compruebe si el enlace al software desarrollado por el tercero es válido. Lea la descripción del evento.	30 días
Error al instalar las actualizaciones de Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Este tipo de evento ocurre cuando no se pueden instalar las actualizaciones de Windows. Configurar las actualizaciones de Windows en una directiva del Agente de red. 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 se ha completado con una advertencia	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 días
La instalación de la actualización de software de terceros se ha pospuesto	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 días
Ocurrió un problema de seguridad	549	GNRL_EV_APP_INCIDENT_OCCURED	30 días
Se inició el Proxy de KSN. No se pudo comprobar la disponibilidad de KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 días

Eventos del Agente de red: nivel Información

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center Linux que tienen el nivel de gravedad **Información**.

Para cada evento que una aplicación puede generar, puede especificar la configuración de notificación y la configuración de almacenamiento en la pestaña **Configuración de eventos** en la directiva de la aplicación. Si desea configurar los ajustes de notificación para todos los eventos a la vez, configure los ajustes de notificación generales en las propiedades del Servidor de administración.

Eventos del Agente de red: nivel Información

Nombre que se muestra para el tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
La actualización para los módulos de software se instaló correctamente	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 días
Se ha iniciado la instalación de la actualización para los módulos de software	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 días
Se instaló una aplicación	7703	KLNAG_EV_INV_APP_INSTALLED	30 días
Se desinstaló una aplicación	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 días
Se instaló una aplicación supervisada	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 días
Se desinstaló una aplicación supervisada	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 días
Se instaló una aplicación de terceros	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 días
Nuevo dispositivo agregado	7708	KLNAG_EV_DEVICE_ARRIVAL	30 días
Dispositivo eliminado	7709	KLNAG_EV_DEVICE_REMOVE	30 días
Se ha detectado un dispositivo	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 días
Dispositivo autorizado	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 días
Windows Desktop Sharing: el archivo ha sido leído	7712	KLUSRLOG_EV_FILE_READ	30 días
Windows Desktop Sharing: el archivo ha sido modificado	7713	KLUSRLOG_EV_FILE_MODIFIED	30 días
Windows Desktop Sharing: la aplicación ha sido iniciada	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 días
Windows Desktop Sharing: iniciado	7715	KLUSRLOG_EV_WDS_BEGIN	30 días
Windows Desktop Sharing: detenido	7716	KLUSRLOG_EV_WDS_END	30 días
La actualización de software de terceros se ha instalado correctamente	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 días
Se ha iniciado la instalación de la actualización de software de terceros	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 días
El proxy de KSN se ha iniciado. La disponibilidad de KSN se verificó correctamente	7719	KSNPROXY_STARTED_CON_CHK_OK	30 días
El Proxy de KSN se detuvo	7720	KSNPROXY_STOPPED	30 días

Utilización de selecciones de eventos

Las selecciones de eventos brindan una vista en pantalla de distintos conjuntos de eventos, que se toman de la base de datos del Servidor de administración y se identifican con un nombre. Estos conjuntos de eventos se agrupan y clasifican de distintas maneras:

- Por nivel de importancia: **Eventos críticos**, **Errores funcionales**, **Advertencias** y **Eventos informativos**
- Por fecha: **Eventos recientes**
- Por tipo: **Solicitudes de usuario** y **Eventos de auditoría**

Puede usar los ajustes disponibles en la interfaz de Kaspersky Security Center Cloud Console para ver y crear selecciones de eventos definidas por el usuario.

Para acceder a las selecciones de eventos disponibles en Kaspersky Security Center Cloud Console, vaya a la sección **Supervisión e informes** y haga clic en **Selecciones de eventos**.

De manera predeterminada, las selecciones de eventos incluyen información de los últimos siete días.

Kaspersky Security Center Cloud Console tiene un conjunto predeterminado de selecciones de eventos:

- Eventos con distintos niveles de importancia:
  - **Eventos críticos**
  - **Errores funcionales**
  - **Advertencias**
  - **Mensajes de información**
- **Solicitudes de usuario** (eventos de aplicaciones administradas)
- **Eventos recientes** (de la semana anterior)
- Eventos de auditoría

  Kaspersky Security Center Cloud Console le mostrará eventos de auditoría vinculados a las operaciones de servicio que se efectúen en su espacio de trabajo. Tales eventos están condicionados por las acciones que realizan los especialistas de Kaspersky. Estos son algunos ejemplos de esos eventos: cambios en los puertos del Servidor de administración; creación de copias de seguridad de la base de datos del Servidor de administración; y 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 el tiempo que Kaspersky Security Center Cloud Console demora en mostrar los eventos. Cuanto más grande es la base de datos, más lento puede ser el proceso.

Puede hacer lo siguiente:

- Editar propiedades de selecciones de eventos
- Generar selecciones de eventos
- Ver detalles de las selecciones de eventos
- Eliminar selecciones de eventos

- Eliminar eventos de la base de datos del Servidor de administración

Crear una selección de eventos

Para crear una selección de eventos:

1. En el menú principal, vaya a **Supervisión e informes** → **Selecciones de eventos**.
2. Haga clic en **Agregar**.
3. En la ventana **Nueva selección de eventos** que se abre, defina los ajustes de la nueva selección de eventos. Haga esto en una o varias de las secciones de la ventana.
4. Haga clic en **Guardar** para guardar los cambios.

   Se abre la ventana de confirmación.
5. Para ver el resultado de la selección de eventos, deje marcada la casilla **Ir al resultado de la selección**.
6. Haga clic en **Guardar** para confirmar que desea crear la selección de eventos.

Si dejó marcada la casilla **Ir al resultado de la selección**, verá el resultado de la selección de eventos. De lo contrario, encontrará la nueva selección de eventos en la lista de selecciones de eventos.

Editar una selección de eventos

Para editar una selección de eventos:

1. En el menú principal, vaya a **Supervisión e informes** → **Selecciones de eventos**.
2. Marque la casilla ubicada junto a la selección de eventos que desee editar.
3. Haga clic en el botón **Propiedades**.

   Se abrirá una ventana para configurar la selección de eventos.
4. Modifique las propiedades de la selección de eventos.

   > Si eligió una selección de eventos predefinida, solo podrá editar las propiedades disponibles en las pestañas **General** (excepto el nombre de la selección), **Hora** y **Derechos de acceso**.

   Si eligió una selección de eventos definida por el usuario, podrá editar cualquiera de las propiedades.
5. Haga clic en **Guardar** para guardar los cambios.

La selección de eventos editada se muestra en la lista.

Ver una lista de una selección de eventos

Para ver una selección de eventos:

1. En el menú principal, vaya a **Supervisión e informes → Selecciones de eventos**.
2. Marque la casilla ubicada junto a la selección de eventos que desee iniciar.
3. Realice una de las siguientes acciones:
   - Si desea configurar la clasificación en el resultado de la selección de eventos, haga lo siguiente:
     a. Haga clic en el botón **Reconfigurar la clasificación e iniciar**.
     b. Cuando se abra la ventana **Reconfigurar la clasificación para la selección de eventos**, ajuste las opciones de clasificación.
     c. Haga clic en el nombre de la selección.
   - Si, por el contrario, desea ver la lista de eventos tal como están ordenados en el Servidor de administración, haga clic en el nombre de la selección.

Se muestra el resultado de la selección de eventos.

Exportar una selección de eventos

Kaspersky Security Center Cloud Console permite guardar una selección de eventos y su configuración en un archivo KLO. El archivo KLO puede usarse para importar la selección de eventos guardada en Kaspersky Security Center Windows o Kaspersky Security Center Linux.

Tenga en cuenta que solo puede exportar selecciones de eventos definidas por el usuario. Las selecciones de eventos del conjunto predeterminado de Kaspersky Security Center Cloud Console (selecciones predefinidas) no se pueden guardar en un archivo.

Para exportar una selección de eventos:

1. En el menú principal, vaya a **Supervisión e informes → Selecciones de eventos**.
2. Marque la casilla ubicada junto a la selección de eventos que desee exportar.

   No es posible exportar más de una selección de eventos a la vez. Si selecciona más de una selección, el botón **Exportar** se desactivará.
3. Haga clic en el botón **Exportar**.
4. En la ventana abierta **Guardar como**, especifique el nombre y la ruta del archivo de selección de eventos y luego haga clic en el botón **Guardar**.

   La ventana **Guardar como** aparecerá solo si utiliza los navegadores Google Chrome, Microsoft Edge u Opera. Si utiliza otro navegador, el archivo de la selección de eventos se guardará automáticamente en la carpeta **Descargas**.

Importar una selección de eventos

Kaspersky Security Center Cloud Console permite importar una selección de eventos de un archivo KLO. El archivo KLO contiene la selección de eventos exportada y su configuración.

Para importar una selección de eventos:

1. En el menú principal, vaya a **Supervisión e informes** → **Selecciones de eventos**.
2. Haga clic en el botón **Importar** y luego elija un archivo de selección de eventos que desee importar.
3. En la ventana que se abre, especifique la ruta al archivo KLO y haga clic en el botón **Abrir**. Tenga en cuenta que no podrá seleccionar más de un archivo de selección de eventos.

   Comienza el procesamiento de selección de eventos.

Aparecerá una notificación con los resultados de la importación. Si la selección de eventos se importa correctamente, puede hacer clic en el vínculo **Ver detalles de importación** para ver las propiedades de la selección de eventos.

Una vez que se complete la importación, la selección de eventos aparece en la lista de selección. Los ajustes de la selección de eventos también se importan.

Si la selección de eventos importada tiene el mismo nombre que una selección de eventos existente, el nombre de la selección importada se complementa con un índice secuencial en formato **(<siguiente número secuencial>)**, por ejemplo **(1)**, **(2)**.

Ver los detalles de un evento

Para ver los detalles de un evento:

1. Genere una selección de eventos.
2. Haga clic en la hora del evento por el que desee consultar.

   Se abre la ventana **Propiedades del evento**.
3. En la ventana que se abre, puede hacer lo siguiente:
   - Ver la información del evento seleccionado
   - Ir a los eventos que se encuentran antes y después del elegido en el resultado de la selección de eventos
   - Ir al dispositivo en el que ocurrió el evento
   - Ir al grupo de administración del dispositivo en el que ocurrió el evento
   - Si el evento está relacionado con una tarea, ir a las propiedades de esa tarea

Exportar eventos a un archivo

Kaspersky Security Center 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. Marque la casilla ubicada junto al evento pertinente.

   También puede seleccionar varios eventos o la selección de eventos completa.
3. Haga clic en el botón **Exportar a archivo**.

El evento seleccionado se exporta a un archivo TXT.

Acceder al historial de un objeto desde un evento

Puede acceder al historial de revisiones de un objeto compatible con la administración de revisiones desde un evento relacionado con la creación o modificación de ese objeto.

Para acceder al historial de un objeto desde un evento:

1. Genere una selección de eventos.
2. Marque la casilla ubicada junto al evento pertinente.
3. Haga clic en el botón **Historial de revisiones**.

Se abre el historial de revisiones del objeto.

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 eventos de advertencia del Servidor de administración denominado **Se superó el límite del número de eventos en la base de datos, se eliminó los eventos**. 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 lo 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), el número de eventos puede ser demasiado grande y los eventos puede inundar la base de datos. En este caso, se recomienda seleccionar una de dos opciones en la configuración de la tarea:

- **Guardar eventos relacionados con el progreso de la tarea**. En este caso, Kaspersky Security Center Cloud Console almacena solo información sobre el inicio de la tarea, el progreso y la finalización (satisfactoria, con una advertencia o error) de cada dispositivo en el que se ejecuta la tarea.

- **Guardar solo los resultados de la ejecución de la tarea**. En este caso, Kaspersky Security Center Cloud Console solo almacena información sobre la finalización de la tarea (satisfactoria, con una advertencia o error) de cada dispositivo en el que se ejecuta la tarea.

Si se ha definido una directiva para un número bastante grande de dispositivos (por ejemplo, más de 10 000), el número de eventos también puede ser grande y los eventos pueden inundar la base de datos. En este caso, se recomienda elegir solo los eventos más críticos en la configuración de la directiva y habilitar su registro. Se recomienda desactivar el registro de todos los demás eventos.

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 **Supervisión e informes → Selecciones de eventos**.

2. Marque las casillas ubicadas junto a las selecciones de eventos que desee eliminar.

3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic en **Aceptar**.

Se elimina la selección de eventos.

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

Para ayudarlo a supervisar la red de su organización, Kaspersky Security Center Cloud Console puede enviarle notificaciones sobre los eventos que usted considere importantes. Puede configurar el envío de notificaciones por correo electrónico para cualquier evento.

Cada vez que reciba una notificación por correo electrónico, podrá decidir cómo responderá al evento. La respuesta debe ser la que mejor se adecue a 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 **Fijar en Crítico si esto se cumple**, habilite la condición bajo la cual el estado de un dispositivo cambiará a *Crítico*.

   Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.

6. En la lista, seleccione el botón de opción ubicado junto a la condición.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor necesario para la condición seleccionada.

No es posible configurar valores para todas las condiciones.

9. Haga clic en **Aceptar**.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Crítico* al dispositivo administrado.

Para habilitar el cambio de estado a Advertencia para los dispositivos:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Jerarquía de grupos**.
2. En la lista de grupos que se abre, haga clic en el vínculo con el nombre del grupo que contenga los dispositivos para los que desee modificar el cambio de estado.
3. En la ventana de las propiedades que se abre, seleccione la pestaña **Estado del dispositivo**.
4. En el panel izquierdo, seleccione **Advertencia**.
5. En el panel derecho, en la sección **Fijar en Advertencia si esto se cumple**, habilite la condición que hará que el estado de un dispositivo cambie a *Advertencia*.

   Solo podrá modificar los ajustes que no estén bloqueados en la directiva primaria.

6. En la lista, seleccione el botón de opción ubicado junto a la condición.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor necesario para la condición seleccionada.

   No es posible configurar valores para todas las condiciones.

9. Haga clic en **Aceptar**.

Cuando se cumplan las condiciones especificadas, se asignará el estado *Advertencia* al dispositivo administrado.

Configurar el envío de notificaciones

Puede recibir notificaciones por correo electrónico sobre los eventos que ocurren en Kaspersky Security Center Cloud Console.

Para configurar el envío de notificaciones sobre los eventos que ocurren en Kaspersky Security Center Cloud Console, haga lo siguiente:

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

   Se abrirá la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.

2. Haga clic en la sección **Notificación** y luego, en el panel de la derecha, configure los ajustes de las notificaciones por correo electrónico:

   Direcciones de los destinatarios

Las direcciones de correo electrónico a las que se enviarán las notificaciones de Kaspersky Security Center Cloud Console. Puede especificar varias direcciones en este campo, separándolas con punto y coma.

Puede introducir hasta veinticuatro direcciones de correo electrónico.

3. Haga clic en el botón **Enviar mensaje de prueba** para que la aplicación envíe una notificación de prueba a las direcciones de correo electrónico que haya introducido. Con esto, podrá comprobar si las notificaciones se configuraron correctamente.

4. Haga clic en el botón **Aceptar** para cerrar la ventana de propiedades del Servidor de administración.

Los ajustes de envío de notificaciones guardados se aplicarán a todos los eventos que sucedan 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

Puede utilizar la sección de novedades de Kaspersky (**Supervisión e informes → Novedades de Kaspersky**) para mantenerse al tanto de las últimas noticias sobre Kaspersky Security Center Cloud Console y las aplicaciones administradas que utiliza en sus dispositivos administrados. Kaspersky Security Center Cloud Console actualiza periódicamente la información de esta sección; las novedades antiguas se eliminan y se reemplazan con información nueva.

Kaspersky Security Center Cloud Console solo le mostrará novedades que estén relacionadas con el Servidor de administración al que se encuentre conectado o con las aplicaciones de Kaspersky que estén instaladas en los dispositivos administrados por ese Servidor de administración. Las novedades de cada tipo de Servidor de administración (primario, secundario o virtual) se muestran por separado.

Cuando hay más de un administrador que utiliza Kaspersky Security Center Cloud Console y cada cual ha configurado un idioma diferente para la interfaz, Kaspersky Security Center Cloud Console muestra las novedades de Kaspersky en cada idioma utilizado por esas personas. Si cambia el idioma de la interfaz, las novedades de Kaspersky disponibles en el nuevo idioma aparecerán en la sección automáticamente una vez que cierre y vuelva a abrir su sesión en la consola.

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.

Las novedades sobre temas de seguridad no se pueden deshabilitar cuando Kaspersky Security Center Cloud Console opera en modo de prueba.

Para que la información mostrada sea relevante para la configuración de su protección de red, Kaspersky Security Center Cloud Console transmite datos a los servidores de Kaspersky en la nube y recibe solo novedades relacionadas a las aplicaciones de Kaspersky instaladas en su red. Encontrará una descripción de los datos que se pueden transmitir a los servidores en el contrato de Kaspersky Security Center Cloud Console que aceptó al crear un espacio de trabajo para su 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 que la información mostrada le resulte útil para proteger los dispositivos de su red y para llevar a cabo sus tareas diarias, Kaspersky Security Center Cloud Console transmite datos a los servidores de Kaspersky en la nube y recibe las novedades pertinentes. Encontrará una descripción de los datos que se pueden transmitir a los servidores en la sección "Datos procesados" de la Declaración de KSN.

La nueva información se divide en las siguientes categorías, según su importancia:

1. Información crítica
2. Noticias importantes
3. Advertencia
4. Información

Cuando aparece nueva información en la sección de novedades de Kaspersky, Kaspersky Security Center Cloud Console muestra una etiqueta de notificación correspondiente al nivel de importancia de la novedad. Haga clic en la etiqueta para ver la información en la sección de novedades de Kaspersky.

Dejar de recibir las novedades de Kaspersky

La sección Novedades de Kaspersky (**Supervisión e informes → Novedades de Kaspersky**) le permite mantenerse al tanto de las últimas noticias relacionadas con su versión de Kaspersky Security Center Cloud Console y con las aplicaciones administradas que utiliza en sus 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.

Las novedades sobre temas de seguridad no se pueden deshabilitar cuando Kaspersky Security Center Cloud Console opera en modo de prueba.

Para dejar de recibir novedades sobre temas de seguridad:

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

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, vaya a la sección **Novedades de Kaspersky**.

3. Ponga el interruptor en la posición **Novedades sobre seguridad Deshabilitado**.

4. Haga clic en el botón **Guardar**.

   Ya no recibirá novedades de Kaspersky.

Las novedades con fines publicitarios están deshabilitadas de forma predeterminada. Solo recibirá este tipo de novedades si ha habilitado Kaspersky Security Network (KSN). Si quiere deshabilitar las novedades con fines publicitarios, deshabilite KSN.

Para dejar de recibir novedades que tengan fines publicitarios:

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

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, elija la sección **Configuración de KSN**.

3. Deshabilite la opción **Acepto utilizar Kaspersky Security Network**.

4. Haga clic en el botón **Guardar**.

   Ya no recibirá novedades con fines publicitarios.

Recibir una advertencia sobre la caducidad de una licencia

Para agregar una clave de licencia de Kaspersky Endpoint Security for Business Select al Servidor de administración:

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

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **General**, vaya a la sección **Claves de licencia**.

3. Haga clic en **Seleccionar**.

4. En la ventana que se abre, seleccione su licencia y haga clic en **Aceptar**.

   Si no se muestra ninguna licencia, también puede hacer clic en **Agregar nueva clave de licencia** y utilizar un código de activación.

La licencia se agregará al repositorio del Servidor de administración. Con ello, el Servidor de administración generará el evento crítico *La licencia está por caducar* un día antes de que caduque el periodo de vigencia de la licencia, y el evento crítico *Modo de funcionalidad limitada* una vez que caduque la licencia. Si lo desea, puede configurar el envío de notificaciones.

Si agrega una clave de licencia de Kaspersky Endpoint Security for Business Select al repositorio del Servidor de administración, se considerará que la licencia se ha utilizado en un dispositivo.

Cloud Discovery

Kaspersky Security Center Cloud Console le permite supervisar el uso de los servicios en la nube en dispositivos administrados con Windows y bloquear el acceso a los servicios en la nube que considera no deseados. Cloud Discovery monitorea los intentos de los usuarios de acceder a estos servicios desde navegadores y aplicaciones de escritorio. También supervisa los intentos de los usuarios de acceder a servicios en la nube mediante conexiones no cifradas (por ejemplo, a través del protocolo HTTP). La función permite detectar y detener el uso de servicios en la nube por parte de la llamada "TI invisible".

La función Cloud Discovery solo está disponible si compró una licencia de Kaspersky Next. Para obtener más información, consulte Licencias y cantidad mínima de dispositivos para cada licencia.

Puede habilitar la función Cloud Discovery y seleccionar las directivas o los perfiles de seguridad para los que desee habilitar la función. También puede habilitar o deshabilitar la función para cada directiva o perfil de seguridad de forma independiente. Puede bloquear el acceso a los servicios en la nube a los que no desee que accedan los usuarios.

Para poder bloquear el acceso a servicios en la nube no deseados, asegúrese de que se cumplan los siguientes requisitos previos:

- Utiliza Kaspersky Endpoint Security 11.2 para Windows o una versión posterior. Las versiones anteriores de la aplicación de seguridad solo permiten supervisar el uso de servicios en la nube.
- Compró una licencia de Kaspersky Next que ofrece la posibilidad de bloquear el acceso a servicios de nube no deseados. Para obtener más información, consulte la Ayuda de Kaspersky Next.

El widget de Cloud Discovery y los informes de Cloud Discovery muestran información sobre los intentos concretados y bloqueados de acceder a servicios en la nube. El widget también muestra el nivel de riesgo de cada servicio en la nube. Kaspersky Security Center 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 habilitada.

Habilitar Cloud Discovery mediante el widget

La función Cloud Discovery permite obtener información sobre el uso de servicios en la nube de todos los dispositivos administrados que se han protegido con directivas de seguridad que tengan la función habilitada. Puede habilitar o deshabilitar Cloud Discovery exclusivamente para la directiva de Kaspersky Endpoint Security para Windows.

Existen dos formas de habilitar la función Cloud Discovery:

- utilizar el widget de Cloud Discovery;
- modificar las propiedades de la directiva de Kaspersky Endpoint Security para Windows.

  Para obtener información detallada sobre cómo habilitar la función Cloud Discovery en las propiedades de la directiva de Kaspersky Endpoint Security para Windows, consulte la sección Cloud Discovery en la Ayuda de Kaspersky Endpoint Security para Windows.

Tenga en cuenta que la función Cloud Discovery solo se puede deshabilitar en los ajustes de la directiva de Kaspersky Endpoint Security para Windows.

Para habilitar Cloud Discovery, debe tener el derecho **Modificar** en el área funcional **Características generales: funcionalidad básica**.

Para habilitar la función Cloud Discovery mediante el widget:

1. Vaya a Kaspersky Security Center Cloud Console.
2. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
3. En el widget de **Cloud Discovery**, haga clic en el botón **Habilitar**.
4. En la ventana **Habilitar Cloud Discovery** que se abre, seleccione las directivas de seguridad para las que desea habilitar la función y, luego, haga clic en el botón **Habilitar**.

   Los siguientes ajustes de la directiva se habilitarán automáticamente: **Inyectar script en el tráfico web para interactuar con las páginas web**, **Monitor de sesión web** y **Análisis de conexiones cifradas**.

La función Cloud Discovery queda habilitada y el widget se agrega al panel.

Agregar el widget de Cloud Discovery al panel

Puede agregar el widget de **Cloud Discovery** al panel para supervisar el uso de servicios en la nube en los dispositivos administrados.

Para agregar el widget de Cloud Discovery al panel, debe tener el derecho **Modificar** en el área funcional **Características generales: Funcionalidad básica**.

Para agregar el widget de Cloud Discovery al panel:

1. Vaya a Kaspersky Security Center Cloud Console.
2. En el menú principal, vaya a **Supervisión e informes** → **Panel**.
3. Haga clic en el botón **Agregar o restaurar widget web**.
4. En la lista de widgets disponibles, haga clic en el ícono del corchete angular (>) ubicado junto a la categoría **Otro**.
5. Seleccione el widget **Cloud Discovery** y, luego, haga clic en el botón **Agregar**.

   Si la función Cloud Discovery está deshabilitada, siga las instrucciones en la sección "Habilitar Cloud Discovery mediante el widget".

El widget seleccionado se agrega al final del panel.

Ver información sobre el uso de servicios en la nube

Puede ver el widget de **Cloud Discovery**, que muestra información sobre los intentos de acceso a servicios en la nube. El widget también muestra el nivel de riesgo de cada servicio en la nube.
Kaspersky Security Center 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 habilitada.

Antes de acceder a la información, asegúrese de que se cumplan los siguientes requisitos:

- Que el widget de Cloud Discovery se haya agregado al panel.
- Que la función Cloud Discovery esté habilitada.
- Que tenga el derecho de **Leer** en el área funcional **Características generales: funcionalidad básica**.

Para ver el widget de Cloud Discovery:

1. Vaya a Kaspersky Security Center Cloud Console.
2. En el menú principal, vaya a **Supervisión e informes** → **Panel**.

   El widget de **Cloud Discovery** se muestra en el panel.
3. En el lado izquierdo del widget de **Cloud Discovery**, seleccione una categoría de servicios en la nube.

   En la tabla ubicada en el lado derecho del widget, se mostrarán hasta cinco servicios de la categoría seleccionada a los que los usuarios intenten acceder con mayor frecuencia. Se cuentan tanto los intentos exitosos como los bloqueados.
4. En el lado derecho del widget, seleccione un servicio específico.

   En la tabla que verá a continuación, se mostrarán los diez dispositivos que hayan intentado acceder a un servicio con mayor frecuencia. Puede usar esta tabla para generar dos tipos de informes: un informe sobre los intentos de acceso exitosos y un informe sobre los intentos de acceso bloqueados.

   Además, en esta tabla puede bloquear el acceso a un servicio en la nube para un dispositivo específico.

El widget mostrará la información solicitada.

En el widget que se abre, puede hacer lo siguiente:

- dirigirse a la sección **Supervisión e informes** → **Informes** para ver los informes de Cloud Discovery;
- bloquear o permitir el acceso a un servicio de nube seleccionado.

La función Cloud Discovery solo está disponible si compró una licencia de Kaspersky Next. Para obtener más información, consulte Licencias y cantidad mínima de dispositivos para cada licencia.

Nivel de riesgo de un servicio en la nube

Cloud Discovery indica un nivel de riesgo para cada servicio en la nube. El nivel de riesgo ayuda a determinar qué servicios no se ajustan a los requisitos de seguridad de la organización. Posiblemente quiera tener en cuenta el nivel de riesgo a la hora de decidir si bloqueará el acceso a un determinado servicio.

El nivel de riesgo es un índice estimado; no indica la calidad de un servicio en la nube o del proveedor del servicio. El nivel de riesgo es simplemente una recomendación de los expertos de Kaspersky.

Los niveles de riesgo de los servicios en la nube se muestran en el widget de Cloud Discovery y en la lista de todos los servicios en la nube supervisados.

Bloquear el acceso a servicios en la nube no deseados

Puede bloquear el acceso a los servicios en la nube a los que no desee que accedan los usuarios. También puede permitir el acceso a servicios en la nube que se encuentren bloqueados.

Al decidir si bloqueará el acceso a un servicio determinado, entre otras consideraciones, es posible que desee tener en cuenta el nivel de riesgo.

El acceso a los servicios en la nube puede bloquearse o permitirse en una directiva o en un perfil de seguridad.

Existen dos formas de bloquear el acceso a servicios en la nube no deseados:

- Utilizar el widget de Cloud Discovery.

  Si elige esta opción, puede bloquear el acceso a servicios individuales.

- Modificar las propiedades de la directiva de Kaspersky Endpoint Security para Windows.

  Si elige esta opción, puede bloquear el acceso a servicios individuales o incluso a categorías completas.

  Para obtener información detallada sobre cómo habilitar la función Cloud Discovery en las propiedades de la directiva de Kaspersky Endpoint Security para Windows, consulte la sección Cloud Discovery en la Ayuda de Kaspersky Endpoint Security para Windows.

Para bloquear o permitir el acceso a un servicio en la nube mediante el widget:

1. Abra el widget de Cloud Discovery y seleccione el servicio en la nube en cuestión.
2. En el panel **Los 10 principales dispositivos que utilizan el servicio**, busque la directiva o el perfil de seguridad en que desee bloquear o permitir el servicio.
3. En la línea correspondiente, en la columna **Estado del acceso en la directiva o el perfil**, realice una de las siguientes acciones:
   - Para bloquear el servicio, seleccione **Bloqueado** en la lista desplegable.
   - Para permitir el servicio, seleccione **Permitido** en la lista desplegable.
4. Haga clic en el botón **Guardar**.

El acceso al servicio seleccionado queda bloqueado o permitido en la directiva o el perfil de seguridad.

Diagnóstico remoto de dispositivos cliente

Puede usar la función de diagnóstico remoto para realizar a distancia las siguientes operaciones en dispositivos cliente basados en Windows y Linux:

- Habilitar y deshabilitar la característica de seguimiento, cambiar el nivel de seguimiento y descargar el archivo de seguimiento
- Descargar información del sistema y los ajustes de las aplicaciones
- Descargar registros de eventos
- Crear un archivo de volcado para una aplicación
- Realizar un diagnóstico y descargar el informe de diagnóstico
- Iniciar, detener y reiniciar aplicaciones

Puede utilizar los registros de eventos y los informes de diagnóstico descargados de un dispositivo cliente para solucionar problemas por cuenta propia. Si se comunica con el servicio de soporte técnico de Kaspersky, los especialistas podrían pedirle que descargue archivos de seguimiento, archivos de volcado, registros de eventos e informes de diagnóstico del dispositivo cliente para que sean analizados en Kaspersky.

Abrir la ventana de diagnóstico remoto

Para realizar un diagnóstico remoto de dispositivos cliente basados en Windows y Linux, debe abrir la ventana de diagnóstico remoto.

Para abrir la ventana de diagnóstico remoto:

1. Realice una de las siguientes acciones para seleccionar el dispositivo para el que desee abrir la ventana de diagnóstico remoto:
   - Si el dispositivo pertenece a un grupo de administración, en el menú principal, vaya a **Activos (dispositivos)** → **Grupos** → **<nombre del grupo>** → **Dispositivos administrados**.
   - Si el dispositivo pertenece al grupo Dispositivos no asignados, en el menú principal, vaya a **Descubrimiento y despliegue** → **Dispositivos no asignados**.
2. Haga clic en el nombre del dispositivo pertinente.
3. En la ventana que se abre, que contendrá las propiedades del dispositivo, elija la pestaña **Avanzado**.
4. En la pestaña **Avanzado**, haga clic en **Diagnóstico remoto**.

   Esto abre la ventana **Diagnóstico remoto** de un dispositivo cliente. Si no se establece la conexión entre el Servidor de administración y el dispositivo cliente, se muestra el mensaje de error.

Como alternativa, si necesita obtener toda la información de diagnóstico sobre un dispositivo cliente basado en Linux a la vez, puede ejecutar el script collect.sh en este dispositivo.

Habilitar y deshabilitar el seguimiento para las aplicaciones

Puede habilitar y deshabilitar el seguimiento para las aplicaciones, incluido el seguimiento con Xperf.

Habilitar y deshabilitar el seguimiento

Para habilitar o deshabilitar el seguimiento en un dispositivo remoto:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
3. En la lista de aplicaciones, seleccione la aplicación para la que desee habilitar o deshabilitar el seguimiento.

   Se abre la lista de opciones de diagnóstico remoto.
4. Si desea habilitar el seguimiento, haga lo siguiente:

   a. En la sección **Seguimiento**, haga clic en **Habilitar seguimiento**.

   b. En la ventana **Modificar nivel de seguimiento**, recomendamos que mantenga los valores de configuración predeterminados. De ser necesario, un especialista del servicio de soporte técnico le indicará cómo modificar la configuración. Las opciones de configuración disponibles son las siguientes:

   - **Nivel de seguimiento**

     El nivel de seguimiento determina qué tan detallado es el archivo de seguimiento.

   - **Seguimiento con rotación**

     La información de seguimiento se sobrescribe para que el archivo de seguimiento no aumente de tamaño desmedidamente. Especifique el número máximo de archivos que se utilizarán para almacenar la información de seguimiento y el tamaño máximo de cada archivo. Una vez que se haya guardado el número máximo de archivos de seguimiento, cada cual con su tamaño máximo, se eliminará el archivo de seguimiento más antiguo para que se pueda guardar un nuevo archivo de seguimiento.

     Esta opción solo está disponible para Kaspersky Endpoint Security.

   c. Haga clic en **Guardar**.

   Se habilita el seguimiento para la aplicación seleccionada. En algunos casos, para habilitar el seguimiento, deberá reiniciar la aplicación de seguridad y su tarea.

   En los dispositivos cliente basados en Linux, el seguimiento del componente Actualizador del agente de Kaspersky Security se regula mediante la configuración del Agente de red. Por lo tanto, las opciones **Habilitar seguimiento** y **Modificar nivel de seguimiento** están deshabilitadas para este componente en dispositivos cliente que ejecutan Linux.
5. Para deshabilitar el seguimiento para la aplicación seleccionada, haga clic en **Deshabilitar seguimiento**.

   Se deshabilita el seguimiento para la aplicación seleccionada.

Habilitar el seguimiento con Xperf

Si utiliza Kaspersky Endpoint Security, un especialista de nuestro servicio de soporte técnico podría pedirle que habilite el seguimiento con Xperf. Esta función permite obtener información sobre el rendimiento del sistema.

Para habilitar y configurar el seguimiento con Xperf o deshabilitarlo, siga los siguientes pasos:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
3. En la lista de aplicaciones, seleccione Kaspersky Endpoint Security para Windows.

   Se muestra la lista de opciones de diagnóstico remoto para la app Kaspersky Endpoint Security para Windows.
4. En la sección **Seguimiento con Xperf**, haga clic en **Habilitar seguimiento con Xperf**.

   Si el seguimiento con Xperf ya está habilitado, verá, en cambio, el botón **Deshabilitar seguimiento con Xperf**. Haga clic en este botón si desea deshabilitar el seguimiento con Xperf para Kaspersky Endpoint Security para Windows.
5. Cuando se abra la ventana **Cambiar el nivel de seguimiento con Xperf**, dependiendo de lo que le haya pedido el especialista en soporte técnico, haga lo siguiente:

   a. Seleccione uno de los siguientes niveles de seguimiento:

   - **Nivel bajo**

     Un archivo de seguimiento de este tipo contiene una cantidad mínima de información sobre el sistema.

     Esta opción está seleccionada de forma predeterminada.

   - **Nivel profundo**

     Un archivo de seguimiento de este tipo contiene información más detallada que los archivos de seguimiento que se generan cuando se elige la opción *Nivel bajo*. El especialista en soporte técnico podría pedirle que elija este nivel si la información contenida en un archivo de nivel bajo no basta para evaluar el rendimiento del sistema. Un archivo de seguimiento de *Nivel profundo* contiene distintas clases de información técnica sobre el sistema: información sobre el hardware, el sistema operativo, la lista de procesos y programas iniciados y finalizados, los eventos utilizados para la evaluación del rendimiento, eventos de la Herramienta de evaluación del sistema de Windows y más.

   b. Seleccione uno de los siguientes tipos de seguimiento con Xperf:

   - **Tipo básico**

     La información de seguimiento se obtendrá mientras Kaspersky Endpoint Security esté en funcionamiento.

     Esta opción está seleccionada de forma predeterminada.

   - **Tipo con reinicio**

La información de seguimiento se obtendrá cuando se inicie el sistema operativo del dispositivo administrado. Este tipo de seguimiento es efectivo cuando el problema que afecta al rendimiento del sistema ocurre después de encender el dispositivo y antes de que se inicie Kaspersky Endpoint Security.

También podrían pedirle que habilite la opción **Tamaño de archivos de rotación, en MB** para evitar que el archivo de seguimiento aumente de tamaño desmedidamente. Si habilita esta opción, especifique el tamaño que el archivo de seguimiento podrá tener como máximo. Cuando el archivo alcance su máximo tamaño, la información de seguimiento más antigua comenzará a reemplazarse con información nueva.

c. Defina el tamaño del archivo de rotación.

d. Haga clic en **Guardar**.

El seguimiento con Xperf queda configurado y habilitado.

6. Si desea deshabilitar el seguimiento con Xperf para Kaspersky Endpoint Security para Windows, haga clic en **Deshabilitar seguimiento con Xperf** en la sección **Seguimiento con Xperf**.

   Se deshabilita el seguimiento con Xperf.

Descargar los archivos de seguimiento de una aplicación

Para poder descargar archivos de seguimiento de un dispositivo cliente, se debe cumplir alguna de estas condiciones: la opción **No desconectar del Servidor de administración** debe estar habilitada en la configuración del dispositivo o se debe estar usando un servidor push o una puerta de enlace de conexión. Si no se cumplen estas condiciones, no podrá realizar la descarga.

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 desee descargar un archivo de seguimiento.

4. En la sección **Seguimiento**, haga clic en el botón **Archivos de seguimiento**.

   Se abre la ventana **Registros de seguimiento del dispositivo**, en la que se muestra una lista de archivos de seguimiento.

5. En la lista de archivos de seguimiento, seleccione el archivo que desee descargar.

6. Realice una de las siguientes acciones:

   - Si desea descargar el archivo seleccionado, haga clic en **Descargar**. Puede seleccionar uno o varios archivos para descargar.

- Si desea descargar una parte del archivo seleccionado, haga lo siguiente:

  a. Haga clic en **Descargar una parte**.

  No puede descargar partes de varios archivos al mismo tiempo. Si selecciona más de un archivo de seguimiento, se deshabilita el botón **Descargar una parte**.

  b. En la ventana que se abre, indique el nombre y la parte del archivo que desee descargar.

  Para dispositivos basados en Linux, no está disponible la edición del nombre de la parte del archivo.

  c. Haga clic en **Descargar.**

El archivo seleccionado, o la parte seleccionada, se descargará en la ubicación que especifique.

Eliminar archivos de seguimiento

Puede eliminar los archivos de seguimiento que ya no necesite.

Para eliminar un archivo de seguimiento:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto que se abre, seleccione la pestaña **Registros de eventos**.
3. En la sección **Archivos de seguimiento**, haga clic en **Registros de Windows Update** o en **Registros de instalación remota**, dependiendo de cuáles sean los archivos de seguimiento que desee eliminar.

   Se abre la ventana **Registros de seguimiento del dispositivo**, en la que se muestra una lista de archivos de seguimiento.
4. En la lista de archivos de seguimiento, seleccione uno o varios archivos que desee eliminar.
5. Haga clic en el botón **Eliminar**.

Los archivo de seguimiento seleccionados se eliminan.

Descargar la configuración de las aplicaciones

Para poder descargar la configuración de la aplicación de un dispositivo cliente, se debe cumplir alguna de estas condiciones: la opción **No desconectar del Servidor de administración** debe estar habilitada en la configuración del dispositivo o se debe estar usando un servidor push o una puerta de enlace de conexión. Si no se cumplen estas condiciones, no podrá realizar la descarga.

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 las aplicaciones**, haga clic en el botón **Descargar** para descargar la información sobre la configuración de las aplicaciones instaladas en el dispositivo cliente.

En la ubicación especificada, se descarga el archivo ZIP con la información.

Descargar información del sistema desde un dispositivo cliente

Para poder descargar la información del sistema en su dispositivo de un dispositivo cliente, se debe cumplir alguna de estas condiciones: la opción **No desconectar del Servidor de administración** debe estar habilitada en la configuración del dispositivo o se debe estar usando un servidor push o una puerta de enlace de conexión. Si no se cumplen estas condiciones, no podrá realizar la descarga.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

Para descargar la información del sistema de un dispositivo cliente, siga los siguientes pasos:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Información del sistema**.
3. Haga clic en el botón **Descargar** para descargar la información del sistema sobre el dispositivo cliente.

En la ubicación especificada, se descarga el archivo con la información.

Descargar registros de eventos

Para poder descargar los registros de eventos de un dispositivo cliente, se debe cumplir alguna de estas condiciones: la opción **No desconectar del Servidor de administración** debe estar habilitada en la configuración del dispositivo o se debe estar usando un servidor push o una puerta de enlace de conexión. Si no se cumplen estas condiciones, no podrá realizar la descarga.

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 que desee descargar.
4. Realice una de las siguientes acciones:

   - Si desea descargar el archivo de registro seleccionado, haga clic en **Descargar archivo completo**.
   - Si desea descargar una parte del archivo de registro seleccionado, haga lo siguiente:

     a. Haga clic en **Descargar una parte**.

     No puede descargar partes de varios registros al mismo tiempo. Si selecciona más de un registro de eventos, se deshabilita el botón **Descargar una parte**.

b. En la ventana que se abre, indique el nombre y la parte del registro que desee descargar.

c. Haga clic en **Descargar**.

El registro de eventos seleccionado, o la parte seleccionada, se descarga en la ubicación especificada.

Iniciar, detener o reiniciar la aplicación

Puede iniciar, detener y reiniciar las aplicaciones instaladas en los dispositivos cliente.

Para iniciar, detener o reiniciar una aplicación:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, seleccione la pestaña **Aplicaciones de Kaspersky**.

   En la sección **Administración de aplicaciones**, se muestra la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
3. En la lista de aplicaciones, seleccione la aplicación que desee iniciar, detener o reiniciar.
4. Haga clic en uno de los siguientes botones para realizar la acción correspondiente:

   - **Detener la aplicación**

     Este botón solo estará disponible si la aplicación se encuentra en ejecución.
   - **Reiniciar aplicación**

     Este botón solo estará disponible si la aplicación se encuentra en ejecución.
   - **Iniciar la aplicación**

     Este botón solo estará disponible si la aplicación no se encuentra en ejecución.

Dependiendo de la acción que haya elegido, la aplicación seleccionada se iniciará, se detendrá o se reiniciará en el dispositivo cliente.

Si elige reiniciar el Agente de red, se le advertirá que la conexión entre el dispositivo y el Servidor de administración se cerrará.

Realizar un diagnóstico remoto 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 diagnóstico**.

Se iniciará el proceso de diagnóstico remoto y se generará un informe con el resultado. Cuando se complete el proceso, la aplicación le permitirá hacer clic en el botón **Descargar informe de diagnóstico**.

5. Haga clic en el botón **Descargar informe de diagnóstico** para descargar el informe.

En la ubicación especificada, se descarga el archivo.

Ejecutar una aplicación en un dispositivo cliente

Ocasionalmente, 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:

  ```
  echo some result > $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**, seleccione el tipo de objeto que desea cargar:

   - Seleccione **Archivo** para cargar el archivo ejecutable.

   - Seleccione **Carpeta** para cargar la carpeta que contiene la aplicación que desea ejecutar en el dispositivo cliente.

     Si selecciona 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.

   - Seleccione **Archivo comprimido** para cargar el archivo ZIP que contiene la aplicación que desea ejecutar en el dispositivo cliente.

     Si selecciona 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 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 ejecuta en un dispositivo remoto.

4. Para cargar el objeto, selecciónelo en la ventana del sistema o arrástrelo al campo de carga.

5. Si es necesario, en el campo **Argumentos para 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 seleccionada en un dispositivo cliente.

7. Una vez completada con éxito la ejecución de la aplicación, descargue los resultados 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 completó el diagnóstico remoto del dispositivo cliente mediante la aplicación.

Crear un archivo de volcado para una aplicación

El archivo de volcado de una aplicación le permite ver los parámetros de la aplicación que se ejecuta en un dispositivo cliente en un momento determinado. Este archivo también contiene información sobre los módulos que se cargaron para una aplicación.

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 característica no es compatible.

Si desea crear un archivo de volcado para una aplicación:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto, haga clic en la pestaña **Ejecución de una aplicación remota**.
3. En la sección **Generación de un volcado de memoria del proceso**, especifique el archivo ejecutable de la aplicación para la que desea generar un archivo de volcado.
4. Haga clic en el botón **Descargar** para guardar el archivo de volcado para la aplicación especificada.

   Si la aplicación especificada no se está ejecutando en el dispositivo cliente, se muestra el 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. Como alternativa, puede obtener información de diagnóstico sobre un dispositivo basado en Linux utilizando el script collect.sh de Kaspersky. Este script se ejecuta en el dispositivo cliente basado en Linux que necesita ser diagnosticado y luego genera un archivo con la información de diagnóstico, la información del sistema sobre este dispositivo, archivos de seguimiento de aplicaciones, registros del dispositivo y un archivo de volcado para emergencias. aplicaciones terminadas.

Le recomendamos que utilice el script collect.sh para obtener toda la información de diagnóstico sobre el dispositivo cliente basado en Linux a la vez. Si descarga la información de diagnóstico de forma remota a través de Kaspersky Security Center 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 mediante el script collect.sh:

1. Descargue el script collect.sh comprimido en el archivo collect.tar.gz.
2. Copie el archivo descargado en el dispositivo cliente basado en Linux que necesita ser diagnosticado.
3. Ejecute el siguiente comando para descomprimir el archivo collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Ejecute el siguiente comando para especificar los derechos de ejecución del script:

   ```
   # chmod +x collect.sh
   ```

5. Ejecute el script collect.sh utilizando una cuenta con derechos de administrador:

   ```
   # ./collect.sh
   ```

Se genera un archivo con la información de diagnóstico y se guarda en la carpeta /tmp/$HOST_NAME-collect.tar.gz.

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

En esta sección, se describen las etapas que se deben completar para configurar la exportación de eventos del Servidor de administración a un sistema SIEM externo. Si configura este mecanismo de exportación, el administrador del sistema SIEM podrá responder oportunamente a los sucesos del sistema de seguridad que se registren en un dispositivo o grupos de dispositivos administrados.

Requisitos previos

Antes de configurar la exportación de eventos en Kaspersky Security Center Cloud Console, haga lo siguiente:

- Lea sobre los métodos disponibles para exportar eventos.
- Asegúrese de contar con los valores de la configuración del sistema.

Los pasos aquí descritos pueden realizarse en cualquier orden.

Etapas

El proceso para configurar la exportación de eventos a un sistema SIEM se divide en estas etapas:

- **Configurar el sistema SIEM para que reciba los eventos de Kaspersky Security Center Cloud Console**

  Debe configurar la recepción de eventos de Kaspersky Security Center Cloud Console en el sistema SIEM.

- **Marcar los eventos que se van a exportar**

  Debe marcar los eventos que se exportarán 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 aplicaciones administradas de Kaspersky específicas.

- **Configurar Kaspersky Security Center Cloud Console para exportar eventos a un sistema SIEM**

  Debe configurar Kaspersky Security Center Cloud Console para que comience a exportar los eventos al sistema SIEM.

Resultados

Después de configurar la exportación de eventos al sistema SIEM, si seleccionó los eventos que desea exportar, podrá ver los resultados de la exportación.

Antes de comenzar

Para configurar la exportación automática de eventos en Kaspersky Security Center Cloud Console, necesitará especificar algunos parámetros del sistema SIEM. Recomendamos que averigüe los valores de estos parámetros de antemano, antes de comenzar con la configuración de 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 del puerto que se usará para establecer la conexión entre Kaspersky Security Center Cloud Console y el servidor del sistema SIEM. Deberá indicar este valor en la configuración de Kaspersky Security Center Cloud Console y en los ajustes de recepción del sistema SIEM.

- **Protocolo**

  El protocolo que se usará para transferir los mensajes de Kaspersky Security Center Cloud Console al sistema SIEM. Deberá indicar este valor en la configuración de Kaspersky Security Center Cloud Console y en los ajustes de recepción del sistema SIEM.

Acerca de la exportación de eventos

Kaspersky Security Center Cloud Console permite recibir información sobre los eventos que ocurren en el Servidor de administración y en las aplicaciones de Kaspersky que se instalan 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 exportación de eventos de Kaspersky Security Center Cloud Console a un sistema SIEM involucra dos participantes: un remitente de eventos (Kaspersky Security Center Cloud Console) y un receptor de eventos (el sistema SIEM). Para que los eventos se exporten correctamente, tanto el sistema SIEM como Kaspersky Security Center Cloud Console deben contar con la información del otro participante. No importa cuál de los dos lados se configura primero. Puede configurar primero la transmisión de eventos en Kaspersky Security Center Cloud Console y luego su recepción en el sistema SIEM, o viceversa.

Exportación de eventos en formato Syslog

Puede enviar eventos en formato Syslog a cualquier sistema SIEM. Utilizando el formato Syslog, podrá transmitir cualquier evento que ocurra en el Servidor de administración o en las aplicaciones de Kaspersky de los 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 procesar los eventos de 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.

Configurar la exportación de eventos en un sistema SIEM

El proceso de exportación de eventos de Kaspersky Security Center Cloud Console a un sistema SIEM involucra dos participantes: un remitente de eventos (Kaspersky Security Center Cloud Console) y un receptor de eventos (el sistema SIEM). La exportación de eventos debe configurarse tanto en el sistema SIEM como 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 recibir los eventos transmitidos por Kaspersky Security Center Cloud Console, se necesita configurar un receptor en el sistema SIEM. Por lo general, deberá especificar los valores de los siguientes parámetros dentro del sistema SIEM:

- **Puerto**

  Indique el número de puerto utilizado para conectarse a Kaspersky Security Center Cloud Console. El puerto debe ser el mismo que haya especificado en Kaspersky Security Center Cloud Console al configurar la exportación al sistema SIEM.

- **Protocolo de mensajes o tipo de origen**

  Elija el formato Syslog.

Según el sistema SIEM que utilice, deberá configurar algunas opciones adicionales del receptor.

Analizadores de mensajes

Los eventos exportados se transfieren al sistema SIEM en forma de mensajes. Estos mensajes deben analizarse; de lo contrario, el sistema SIEM no puede hacer uso de la información de los eventos. Los analizadores de mensajes son parte del sistema SIEM; están diseñados para leer el contenido de cada mensaje y extraer de este los campos relevantes (id. del evento, gravedad, descripción, parámetros, etc.). El análisis permite que el sistema SIEM procese los eventos que recibe de Kaspersky Security Center Cloud Console y que los almacene en su base de datos.

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. marque las casillas ubicadas al lado de los eventos que quiera exportar a un sistema SIEM.

5. Haga clic en el botón **Marcar para exportar al sistema SIEM mediante Syslog**.

   > También puede marcar un evento para exportarlo a un sistema SIEM en la sección **Registro de los eventos**, que se abre al hacer clic en el vínculo del evento.

6. Aparecerá una marca de verificación (✓) en la columna **Syslog** del evento (o los eventos) que haya elegido exportar al sistema SIEM.

7. Haga clic en el botón **Guardar**.

Los eventos marcados desde la aplicación administrada están listos para ser exportados a un sistema SIEM.

Puede marcar los eventos que desea exportar a un sistema SIEM para un dispositivo administrado específico. Si se marcaron eventos previamente exportados en una directiva de aplicación, no podrá redefinir los eventos marcados para un dispositivo administrado.

Para marcar los eventos que desea exportar a un dispositivo administrado, haga lo siguiente:

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

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el vínculo con el nombre del dispositivo pertinente.

   Se muestra la ventana de propiedades del dispositivo seleccionado.

3. Vaya a la sección **Aplicaciones**.

4. En la lista de aplicaciones, haga clic en el vínculo con el nombre de la aplicación en cuestión.

5. Vaya a la sección **Configuración de eventos**.

6. Active las casillas de verificación ubicadas junto a los eventos que deban exportarse al sistema SIEM.

7. Haga clic en el botón **Marcar para exportar al sistema SIEM mediante Syslog**.

   También puede marcar un evento para exportarlo a un sistema SIEM en la sección **Registro de los eventos**, que se abre al hacer clic en el vínculo del evento.

8. Aparecerá una marca de verificación (✓) en la columna **Syslog** del evento (o los eventos) que haya elegido exportar al sistema SIEM.

En lo sucesivo, si la exportación a un sistema SIEM está configurada, el Servidor de administración enviará los eventos marcados a ese sistema SIEM.

Marcar eventos generales para que se los exporte en formato Syslog

Si lo desea, puede marcar eventos generales para que el Servidor de administración los exporte a sistemas SIEM en formato Syslog.

Para marcar eventos generales y exportarlos a un sistema SIEM:

1. Realice una de las siguientes acciones:

   - En el menú principal, haga clic en el icono de configuración (⚙) ubicado junto al nombre del Servidor de administración pertinente.
   - En el menú principal, vaya a **Activos (dispositivos)** → **Directivas y perfiles** y haga clic en el vínculo de una directiva.

2. En la ventana que se abre, vaya a la pestaña **Configuración de eventos**.

3. Haga clic en **Marcar para exportar al sistema SIEM mediante Syslog**.

   Como alternativa, para marcar un evento que desee exportar al sistema SIEM, puede utilizar la sección **Registro de los eventos** que se abre al hacer clic en el vínculo del evento en cuestión.

4. Aparecerá una marca de verificación (✓) en la columna **Syslog** del evento (o los eventos) que haya elegido exportar al sistema SIEM.

En lo sucesivo, si la exportación a un sistema SIEM está configurada, el Servidor de administración enviará los eventos marcados a ese sistema SIEM.

Acerca de la exportación de eventos en formato Syslog

Los eventos del Servidor de administración y los eventos de las aplicaciones de Kaspersky que se encuentran instaladas en los dispositivos administrados se pueden exportar a un sistema SIEM en formato Syslog.

Syslog es un protocolo de registro de mensajes estándar. Permite que el software que genera los mensajes, el sistema que los almacena y el software que los reporta y analiza sean entidades separadas. Cada mensaje se etiqueta con un código numérico que indica el tipo de software que lo ha generado. A cada mensaje se le asigna, además, un nivel de gravedad.

La definición del formato Syslog se encuentra publicada en documentos RFC del Grupo de Trabajo de Ingeniería de Internet o IETF (estándares de Internet). Para exportar los eventos de Kaspersky Security Center Cloud Console a un sistema externo, se utiliza el estándar RFC 5424.

Kaspersky Security Center Cloud Console permite configurar la exportación de eventos a un sistema externo en formato Syslog.

El proceso de exportación consta de dos pasos:

1. Habilitar la exportación de eventos automática. Este paso consiste en configurar Kaspersky Security Center Cloud Console para que transmita eventos al sistema SIEM. Kaspersky Security Center Cloud Console empezará a enviar los eventos pertinentes en cuanto usted habilite la exportación automática.

2. Seleccionar los eventos que se exportarán al sistema externo. Este paso consiste en indicar cuáles eventos deberán exportarse al sistema SIEM.

Configurar Kaspersky Security Center Cloud Console para exportar eventos a un sistema SIEM

Si desea exportar eventos a un sistema SIEM, debe configurar el proceso de exportación en Kaspersky Security Center Cloud Console.

Para configurar la exportación de eventos a un sistema 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 click en el enlace **Configuración**.

   Se abre la sección **Exportar configuración**.

4. En la sección **Exportar configuración**, configure los siguientes ajustes:

   - Dirección del servidor del sistema SIEM

La dirección IP del servidor en el que está instalado el sistema SIEM. Encontrará este valor en la configuración del sistema SIEM.

- **Puerto del sistema SIEM**

  El número del puerto que se usará para establecer la conexión entre Kaspersky Security Center Cloud Console y el servidor del sistema SIEM. Deberá indicar este valor en la configuración de Kaspersky Security Center Cloud Console y en los ajustes de recepción del sistema SIEM.

- **Protocolo**

Para transmitir mensajes al sistema SIEM, solamente puede usar el protocolo TLS sobre TCP. Para hacer 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 completa de certificados (incluyendo el certificado raíz) de una entidad de certificación (CA) confiable y subir el archivo a Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console verificará si el certificado del servidor SIEM también ha sido (o no) firmado por una entidad de certificación de confianza.

    Para agregar un certificado de confianza, haga clic en el botón **Buscar archivo de certificados de CA** y, a continuación, cargue el certificado en cuestión.

  - **Huellas digitales SHA**. Puede especificar las huellas digitales SHA1 de la cadena de certificados completa del sistema SIEM (incluido el certificado raíz) en Kaspersky Security Center Cloud Console. Para agregar una huella digital SHA1, cópiela en el campo **Huellas digitales** y haga clic en el botón **Agregar**.

  La opción **Agregar autenticación del cliente** permite generar un certificado para autenticar a Kaspersky Security Center Cloud Console. Si utiliza esta opción, 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.

- **Agregar nombre del sujeto / nombre alternativo del sujeto**

  Se denomina "nombre del sujeto" al nombre de dominio para el que se ha obtenido un certificado. Para que Kaspersky Security Center Cloud Console pueda conectarse al servidor del sistema SIEM, el nombre de dominio del servidor del sistema SIEM debe aparecer como nombre del sujeto en el certificado del servidor del sistema SIEM. El servidor del sistema SIEM puede cambiar de nombre de dominio si se modifica también el nombre del sujeto en el certificado. Si se presenta esta situación, utilice el campo **Agregar nombre del sujeto / nombre alternativo del sujeto** para especificar los nombres de sujeto pertinentes. Si alguno de los nombres de sujeto indicados en el campo coincide con el nombre de sujeto especificado en el certificado del sistema SIEM, Kaspersky Security Center Cloud Console considerará que el certificado es válido.

- **Agregar autenticación del cliente**

  Para la autenticación del cliente, puede utilizar su propio certificado o generar uno en Kaspersky Security Center 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**. Use el campo **Archivo con certificado** para cargar el archivo que contenga el certificado y el campo **Archivo con clave** para cargar un archivo que contenga la clave privada. Los archivos no dependen el uno del otro y no importa el orden en que se los carga. Tras cargar los archivos, ingrese la contraseña para decodificar la clave privada en el campo **Verificación de certificado o contraseña**. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

    - **PKCS12 certificado X.509**. Use el campo **Archivo con certificado** para cargar un único archivo que contenga tanto el certificado como su clave privada. Tras cargar el archivo, ingrese la contraseña para decodificar la clave privada en el campo **Verificación de**

certificado o contraseña. Si la clave privada no está codificada, puede dejar la contraseña en blanco.

- **Generar clave**. Puede generar un certificado autofirmado dentro de Kaspersky Security Center Cloud Console. El certificado autofirmado que se genere quedará almacenado en Kaspersky Security Center Cloud Console, y usted podrá transferir la parte pública del certificado o su huella digital SHA-1 al sistema SIEM.

5. Si lo desea, puede exportar eventos que se encuentren archivados en la base de datos del Servidor de administración y definir la fecha a partir de la cual se iniciará la exportación de los eventos archivados:

   a. Haga clic en el 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. Coloque el interruptor en la posición **Exportar eventos a la base de datos del sistema SIEM automáticamente Habilitado**.

7. Para comprobar que la conexión del sistema SIEM se haya configurado correctamente, haga clic en el botón **Comprobar conexión**.

   Se mostrará el estado de la conexión.

8. Haga clic en el botón **Guardar**.

La exportación de eventos al sistema SIEM queda configurada. En lo sucesivo, si la recepción de eventos está configurada en el sistema SIEM, el Servidor de administración exportará los eventos marcados al sistema SIEM. Si definió una fecha de inicio para la exportación, el Servidor de administración también exportará los eventos marcados que se encuentren almacenados desde esa fecha en la base de datos del Servidor de administración.

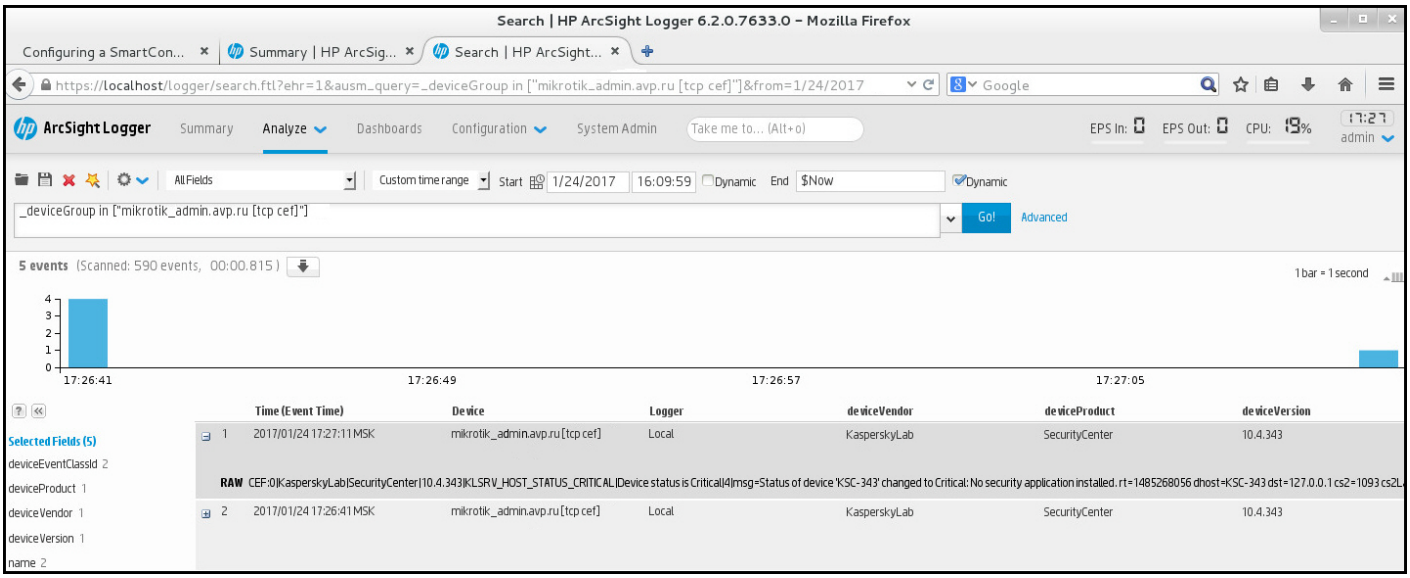
Ver los resultados de la exportación

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 el sistema SIEM recibe y procesa correctamente los eventos que se envían desde Kaspersky Security Center Cloud Console, la configuración de ambos lados es correcta. De no ser este el caso, coteje los ajustes configurados en Kaspersky Security Center Cloud Console con los ajustes configurados en el 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 los administradores que trabajan para un proveedor de servicios administrados (MSP).

Kaspersky Security Center Cloud Console es compatible con el multiinquilinato. Encontrará 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 un equipo o servidor propios. A través de Kaspersky Security Center Cloud Console, el administrador puede instalar las aplicaciones de seguridad de Kaspersky en los dispositivos de una red corporativa, ejecutar tareas de análisis y actualización en forma remota y gestionar las directivas de seguridad de las aplicaciones administradas. También puede usar un panel detallado para conocer rápidamente los estados de los dispositivos corporativos, consultar informes detallados y acceder a ajustes pormenorizados en las directivas de protección.

Características clave de Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console permite hacer lo siguiente:

- Instalar aplicaciones de Kaspersky en los dispositivos de una red y administrar las 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 virtuales y organizarlos en una jerarquía.
- Proteger estaciones de trabajo, servidores y otros dispositivos conectados a la red:
  - Administrar un sistema de protección antimalware basado en las aplicaciones de Kaspersky.
  - Usar prestaciones de detección y respuesta (EDR y MDR) para fines como los siguientes (si se cuenta con una licencia de Kaspersky Endpoint Detection and Response o de Kaspersky Managed Detection and Response):
    - Analizar e investigar incidentes
    - Crear un gráfico con la cadena de desarrollo de la amenaza para visualizar un incidente
    - Aceptar o rechazar respuestas manualmente o configurar la aceptación automática de todas las respuestas
- Usar Kaspersky Security Center Cloud Console como aplicación multiinquilino.
- Administrar de forma remota las aplicaciones de Kaspersky instaladas en los dispositivos cliente.
- Realizar un despliegue centralizado de claves de licencia para las aplicaciones de Kaspersky instaladas en los dispositivos cliente.

- Crear y administrar directivas de seguridad para los dispositivos conectados a la red.
- Crear y administrar cuentas de usuario.
- Crear y administrar roles de usuario (RBAC).
- Crear y administrar tareas para las aplicaciones instaladas en los dispositivos de red.
- Ver informes sobre el estado del sistema de seguridad de cada organización cliente en particular.

Acerca de las licencias de Kaspersky Security Center Cloud Console para los MSP

Cuando comience a usar Kaspersky Security Center Cloud Console, podrá solicitar un espacio de trabajo de prueba (en cuyo caso se le brindará una licencia de prueba de treinta días, que estará integrada en el espacio de trabajo) o podrá ingresar el código de activación de una licencia comercial.

No es posible convertir un espacio de trabajo de prueba en uno comercial. Para continuar usando Kaspersky Security Center Cloud Console después de que caduca una licencia de prueba, se debe eliminar el espacio de trabajo de prueba y se debe crear otro con una licencia comercial.

Más tarde, podrá agregar una o más 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. Si elige integrar las siguientes aplicaciones, por ejemplo, sumará funciones de detección y respuesta a las características de Kaspersky Security Center Cloud Console:

- 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 contra ciberamenazas complejas. Combina tecnologías de autodetección de amenazas con la capacidad de responder a los riesgos encontrados para resistir ataques complejos, como los ataques sin archivo, el abuso de herramientas estándar del sistema y los ataques que permiten montar el ransomware y los nuevos exploits.

  Cuando una aplicación EPP (siglas en inglés de "plataforma de protección de endpoints") desarrollada por Kaspersky detecta un incidente de seguridad, se genera una ficha detallada con información importante sobre el incidente en Kaspersky Security Center Cloud Console. La ficha del incidente es generada por una de estas aplicaciones:

  - Kaspersky Endpoint Agent, software que se instala a la par de la aplicación EPP de Kaspersky
  - Kaspersky Endpoint Security 11.7.0 para Windows, solución que ya trae incorporadas las funciones de EDR Optimum y no obliga a instalar Kaspersky Endpoint Agent

  Puede usar la ficha del incidente para analizar e investigar ese incidente. El incidente también se puede examinar en forma visual, a través de un gráfico que representa la cadena de desarrollo de la amenaza. El gráfico describe las etapas de despliegue del ataque detectado a lo largo del tiempo. Incluye información sobre los módulos involucrados en el ataque y sobre las acciones realizadas por esos módulos.

También puede iniciar una cadena de acciones de respuesta. Puede crear una regla que impida la ejecución de un objeto que no sea de confianza, seleccionar y usar indicadores de vulneración (IOC) para buscar incidentes similares en el grupo de dispositivos, aislar un objeto que no sea de confianza y aislar un dispositivo vulnerado de la red.

Para obtener información acerca de la activación de la aplicación, consulte la documentación de Kaspersky Endpoint Detection and Response Optimum.

Si integra esta aplicación, se agregará la sección **Alertas** a la interfaz de Kaspersky Security Center Cloud Console (**Supervisión e informes** → **Alertas**).

- Kaspersky Managed Detection and Response

  Kaspersky Managed Detection and Response brinda protección ininterrumpida contra el creciente volumen de amenazas que eluden las barreras de seguridad automatizadas de organizaciones que no tienen experiencia, personal o recursos internos suficientes. Los analistas de los centros de operaciones de seguridad (SOC) de MDR de Kaspersky o de una empresa externa investigan los incidentes y ofrecen respuestas para resolverlos. Usted puede aceptar o rechazar manualmente las medidas que se le ofrecen o puede activar una opción para que las respuestas siempre se acepten automáticamente.

  Para obtener más información acerca de la activación de la aplicación, consulte la documentación de Kaspersky Managed Detection and Response.

  Si integra esta aplicación, se agregará la sección **Incidentes** a la interfaz de Kaspersky Security Center Cloud Console (**Supervisión 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 a través de la sección **Opciones de interfaz** de Kaspersky Security Center Cloud Console.

Primeros pasos con 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 se divide en etapas:

1. **Crear una cuenta**

   Para comenzar a usar Kaspersky Security Center Cloud Console, necesitará una cuenta.

   Para crear una cuenta:

   1. Abra su navegador e ingrese a la siguiente dirección: https://ksc.kaspersky.com.
   2. Haga clic en el botón **Crear una cuenta**.
   3. Siga las instrucciones del asistente.

2. **Crear un espacio de trabajo**

   Una vez que tenga su cuenta, puede registrar su empresa y crear un espacio de trabajo.

   Cuando comience a usar Kaspersky Security Center Cloud Console, podrá solicitar un espacio de trabajo de prueba (en cuyo caso se le brindará una licencia de prueba de treinta días, que estará integrada en el espacio de trabajo) o podrá ingresar el código de activación de una licencia comercial.

No es posible convertir un espacio de trabajo de prueba en uno comercial. Para continuar usando Kaspersky Security Center Cloud Console después de que caduca una licencia de prueba, se debe eliminar el espacio de trabajo de prueba y se debe crear otro con una licencia comercial.

Para registrar una empresa y crear un espacio de trabajo:

1. Abra su navegador e ingrese a la siguiente dirección: https://ksc.kaspersky.com.
2. Haga clic en el botón **Iniciar sesión**.
3. Siga las instrucciones del asistente.

3. **Realizar la configuración inicial de Kaspersky Security Center Cloud Console**

   Cuando ingrese al espacio de trabajo creado por primera vez, 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 aplicaciones de Kaspersky. Siga las instrucciones del asistente.

Una vez finalizada la configuración inicial, Kaspersky Security Center Cloud Console está lista para usar.

Recomendaciones para 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:
  - Puede crear un Servidor de administración virtual para los dispositivos de cada cliente (opción recomendada). En este caso, podrá administrar los dispositivos de cada cliente a través de un Servidor de administración virtual independiente de los de sus otros clientes. Al mismo tiempo, contará con el Servidor de administración principal para crear directivas y tareas que sean comunes a todos sus clientes. Los informes generados en el Servidor de administración principal pueden incluir los datos de todos los servidores de administración virtuales.
  - Puede 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 dentro de cada grupo principal. Los grupos subordinados le permitirán, por ejemplo, utilizar configuraciones de protección diferentes para los dispositivos de empleados que trabajen en departamentos diferentes.
- Si ya ha usado Kaspersky Security Center en una infraestructura local, puede migrar los grupos de administración existentes y otros objetos relacionados a Kaspersky Security Center Cloud Console.

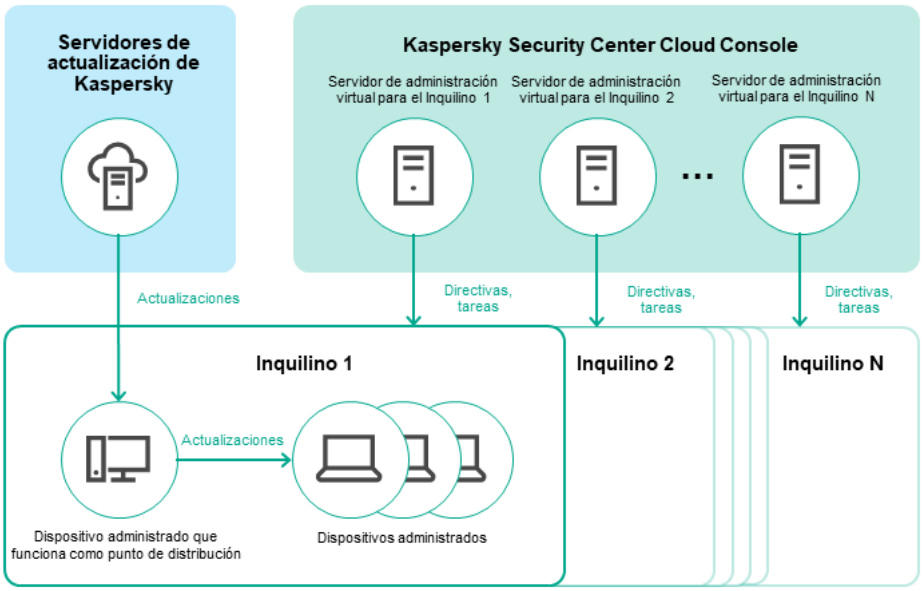
  No es posible migrar servidores de administración virtuales. Una vez que haya migrado sus grupos de administración y demás objetos, podrá crear servidores de administración virtuales en Kaspersky Security Center Cloud Console.

  Procesa a configurar la migración.

El administrador de un Servidor de administración virtual solo puede acceder a ese Servidor virtual desde el Servidor de administración principal. El administrador de un Servidor de administración virtual tiene acceso de lectura a todos los objetos que se crean en el Servidor de administración principal (widgets, informes, roles de usuario, etc.).

Esquema de despliegue típico para los MSP

En esta sección, se describe el esquema de despliegue que los MSP suelen utilizar para administrar varios inquilinos. El esquema se basa en el uso de servidores de administración virtuales independientes para cada inquilino que se deba administrar.



Esquema de despliegue típico para los MSP

El esquema consta de los siguientes componentes principales:

- *Kaspersky Security Center Cloud Console*. Brinda una interfaz de usuario para interactuar con los servicios de administración del espacio de trabajo. Kaspersky Security Center Cloud Console se utiliza para desplegar, administrar y mantener el sistema de protección en 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 virtuales*. Por lo general, el administrador que trabaja para el MSP crea un Servidor de administración virtual para cada inquilino y lo usa para desplegar, administrar y mantener el sistema de protección en la red de la organización cliente correspondiente.

- *Inquilinos*. Organizaciones cliente a las que pertenecen los dispositivos que se deben proteger.

- *Dispositivos administrados*. Dispositivos de la empresa cliente que se encuentran 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 en el que se ha instalado el Agente de red y que se utiliza para distribuir actualizaciones, realizar sondeos de red, instalar aplicaciones en forma remota y recopilar información sobre los equipos asociados a un grupo de administración o a un dominio de difusión. Es tarea del administrador determinar qué dispositivos actuarán como puntos de distribución y designarlos como tales manualmente.

Escenario: Despliegue de la protección (administración de inquilinos mediante servidores de administración virtuales)

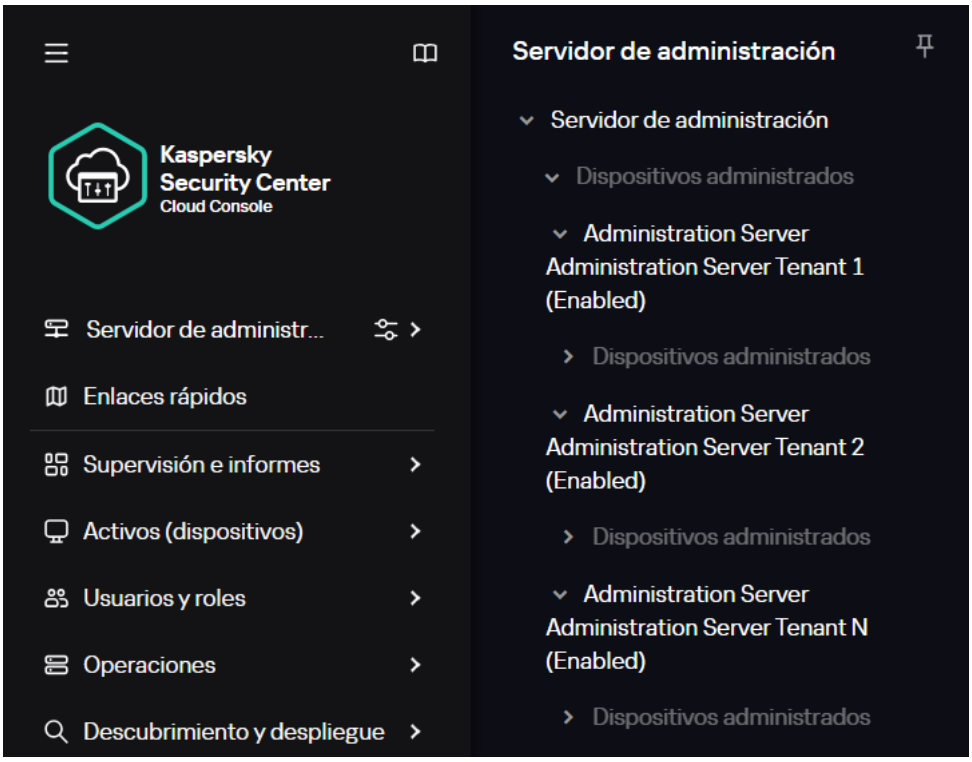
Si nunca ha usado Kaspersky Security Center y desea administrar a sus inquilinos a través de servidores de administración virtuales, siga las instrucciones que se detallan en esta sección. Al concluir el escenario que aquí se describe, los dispositivos de sus clientes estarán protegidos.

Si administra más de un inquilino, repita estos pasos para cada inquilino por separado.

El escenario se divide en etapas:

1. **Crear un Servidor de administración virtual**

   Cree un Servidor de administración virtual para su cliente. El nuevo Servidor de administración virtual aparecerá en la jerarquía de servidores de administración:



Servidores de administración virtuales en la jerarquía de servidores de administración

2. **Seleccionar un dispositivo para que actúe como punto de distribución**

   Decida cuál de los dispositivos del cliente actuará como punto de distribución.

   > No puede haber más de cien puntos de distribución por espacio de trabajo.

3. **Crear 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 de Servidor de administración, puede utilizar el menú principal: haga clic en el ícono del corchete angular ( ) a la derecha del nombre del Servidor de administración con el que esté trabajando y, luego, seleccione el Servidor de administración con el que quiera operar. Cuando esté creando el paquete de instalación independiente, especifique el grupo de administración "Dispositivos administrados" al que quiera mover el dispositivo.

4. **Instalar el Agente de red en el dispositivo seleccionado como punto de distribución**

Utilice el método que le resulte conveniente:

- Instalación manual

  Para transferir el paquete de instalación independiente al dispositivo, puede copiar el paquete en una unidad extraíble (como una unidad flash), colocarlo en una carpeta compartida, etc.

- Despliegue mediante Active Directory

- Despliegue a través de una solución de supervisión y administración remotas (software de RMM)

5. **Designar el punto de distribución**

   Designe el dispositivo en el que acaba de instalar el Agente de red 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 puede realizar sondeos de red utilizando los siguientes métodos:

   - Sondeo de intervalos IP
   - Sondeo de la red de Windows
   - Sondeo de Active Directory

   El sistema sondeará la red siguiendo el cronograma que usted defina. Los dispositivos descubiertos se agregarán al 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 piensa usar un único grupo de administración para administrar los dispositivos del cliente, puede mover los dispositivos al grupo "Dispositivos administrados".

8. **Crear paquetes de instalación para el Agente de red y las aplicaciones de Kaspersky administradas**

   Cree paquetes de instalación para aplicaciones de Kaspersky.

9. **Eliminar 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 las aplicaciones de Kaspersky en los 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.

    Si necesita instalar las aplicaciones de Kaspersky en grupos de administración diferentes o en selecciones de dispositivos diferentes, puede crear varias tareas de instalación remota.

    Tras crear las tareas, puede configurar sus ajustes. Asegúrese de que la programación de cada tarea sea acorde a sus necesidades. La primera tarea de instalación en ejecutarse debe ser la del Agente de red. Una vez que el Agente de red se ha instalado en los dispositivos de sus clientes, puede ejecutarse la tarea para instalar las aplicaciones de Kaspersky administradas.

11. **Verificar el 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 se hayan instalado 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 del Servidor de administración virtual al Servidor de administración principal y, luego, cree una directiva para la aplicación de Kaspersky pertinente.

Escenario: Despliegue de la protección (administración de inquilinos mediante grupos de administración)

Si nunca ha utilizado Kaspersky Security Center y desea administrar sus inquilinos a través de grupos de administración, siga las instrucciones de esta sección. Al concluir el escenario que aquí se describe, los dispositivos de sus clientes estarán protegidos.

El escenario se divide en etapas:

1. **Creación de grupos de administración**

   Cree un grupo de administración para cada uno de sus clientes.

2. **Planificar la estructura de puntos de distribución**

   Decida cuál de los dispositivos de cada cliente actuará como punto de distribución.

   > No puede haber más de cien puntos de distribución por espacio de trabajo.

3. **Crear un paquete de instalación independiente para el Agente de red**

   Cree un paquete de instalación independiente para el Agente de red.

4. **Instalar el Agente de red en los dispositivos que actuarán como puntos de distribución**

   Instale el Agente de red en los dispositivos que haya elegido como puntos de distribución.

   Utilice el método que le resulte conveniente:

   - Instalación manual

     Para transferir el paquete de instalación independiente a los dispositivos, puede copiarlo en una unidad extraíble (como una unidad flash), colocarlo en una carpeta compartida, etc.

   - Despliegue mediante Active Directory

   - Despliegue a través de una solución de supervisión y administración remotas (software de RMM)

5. **Designar los puntos de distribución**

   Indique cuáles dispositivos con el Agente de red actuarán 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 puede realizar sondeos de red utilizando los siguientes métodos:

   - Sondeo de intervalos IP

   - Sondeo de la red de Windows

- Sondeo de Active Directory

El sistema sondeará la red siguiendo el cronograma que usted defina. Los dispositivos descubiertos se agregarán al 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 de Kaspersky administradas**

   Si no utilizó el asistente de inicio rápido o si omitió el paso de creación de paquetes de instalación, cree paquetes de instalación para las aplicaciones de Kaspersky.

9. **Eliminar 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 las 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.

    Si necesita instalar las aplicaciones de Kaspersky en grupos de administración diferentes o en selecciones de dispositivos diferentes, puede crear varias tareas de instalación remota.

    Tras crear las tareas, puede configurar sus ajustes. Asegúrese de que la programación de cada tarea sea acorde a sus necesidades. La primera tarea de instalación en ejecutarse debe ser la del Agente de red. Una vez que el Agente de red se ha instalado en los dispositivos de sus clientes, puede ejecutarse la tarea para instalar las aplicaciones de Kaspersky administradas.

11. **Verificar el 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 se hayan instalado 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 local y Kaspersky Security Center Cloud Console

Si ya ha utilizado Kaspersky Security Center localmente, puede convertir sus servidores de administración locales en servidores de administración secundarios de su nuevo Servidor de administración de Kaspersky Security Center Cloud Console. En esta sección se describe el procedimiento para hacerlo.

Si configura el uso conjunto de Kaspersky Security Center 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:

Agregue sus servidores de administración locales existentes como servidores de administración secundarios.

Licencias de aplicaciones de Kaspersky para los MSP

Kaspersky Security Center Cloud Console permite realizar una distribución centralizada de las claves de licencia para las aplicaciones Kaspersky instaladas en los dispositivos de sus clientes, controlar el uso de estas claves 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. Agregue 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 seleccionará una de las claves de licencia aplicables y la desplegará automáticamente cada vez que se descubra un nuevo dispositivo.
   - Configure la tarea Agregar una clave para distribuir una clave de licencia a los dispositivos.

     Al configurar la tarea, seleccione la clave de licencia que deba desplegarse a los dispositivos y elija el grupo de administración que contenga los dispositivos necesarios.

     Cada tarea puede distribuir una sola clave de licencia. Si necesita distribuir varias claves de licencia, deberá crear una tarea para cada una.

   En este punto, las aplicaciones de Kaspersky instaladas en los dispositivos de sus clientes estarán 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.

Funciones de supervisión y de creación de informes para MSP

Kaspersky Security Center Cloud Console le ofrece al MSP una serie de funciones de supervisión y de creación de informes. Estas prestaciones permiten obtener una visión general de la infraestructura de la organización, ver los estados de protección y acceder a información estadística.

Si ya terminó con el despliegue de Kaspersky Security Center Cloud Console, puede configurar las funciones de supervisión y creación de informes para adaptarlas a sus necesidades.

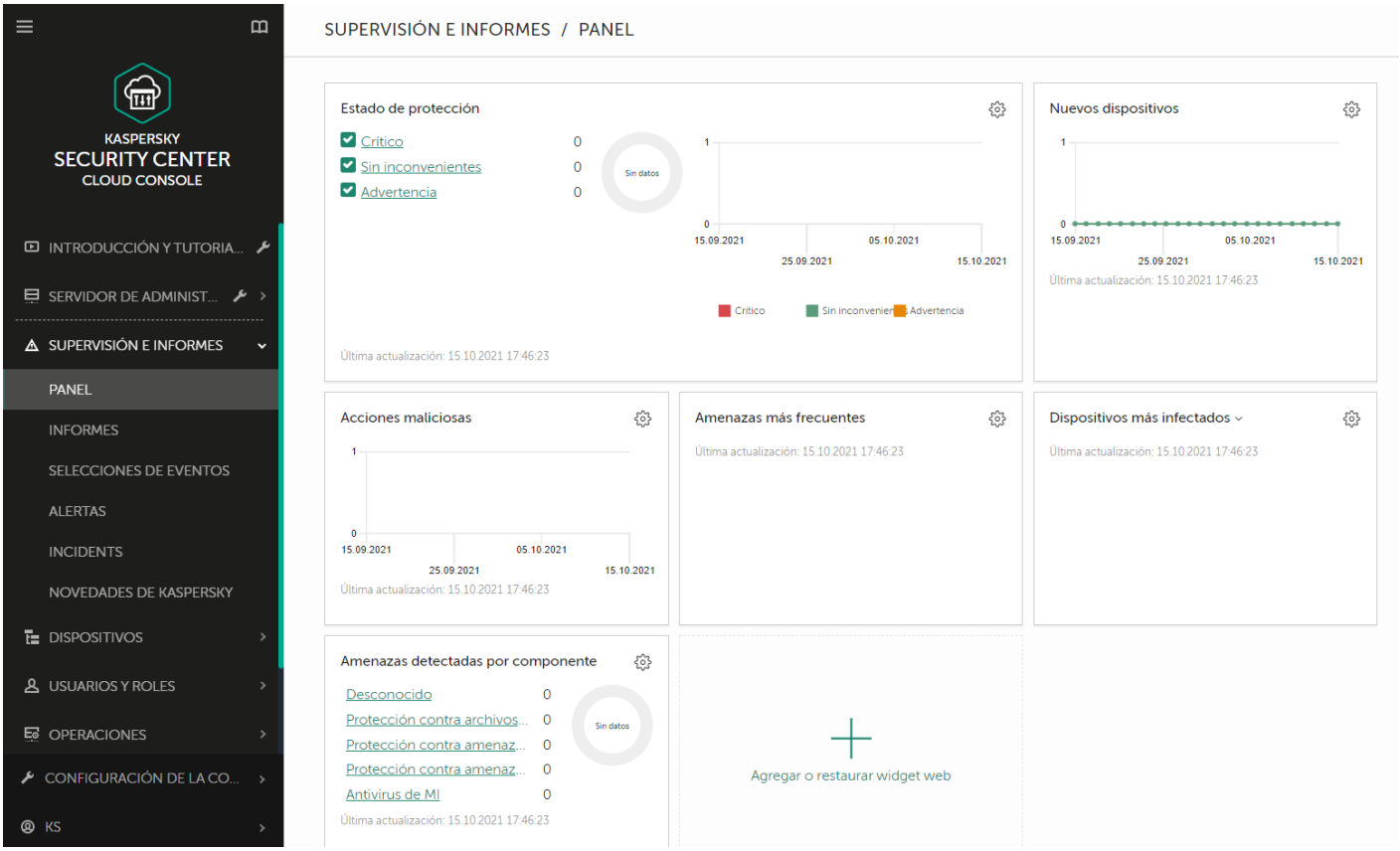
Kaspersky Security Center Cloud Console ofrece las siguientes clases de funciones de supervisión y de trabajo con informes:

- Panel
- Informes

- Selecciones de eventos
- Notificaciones por correo electrónico

Panel

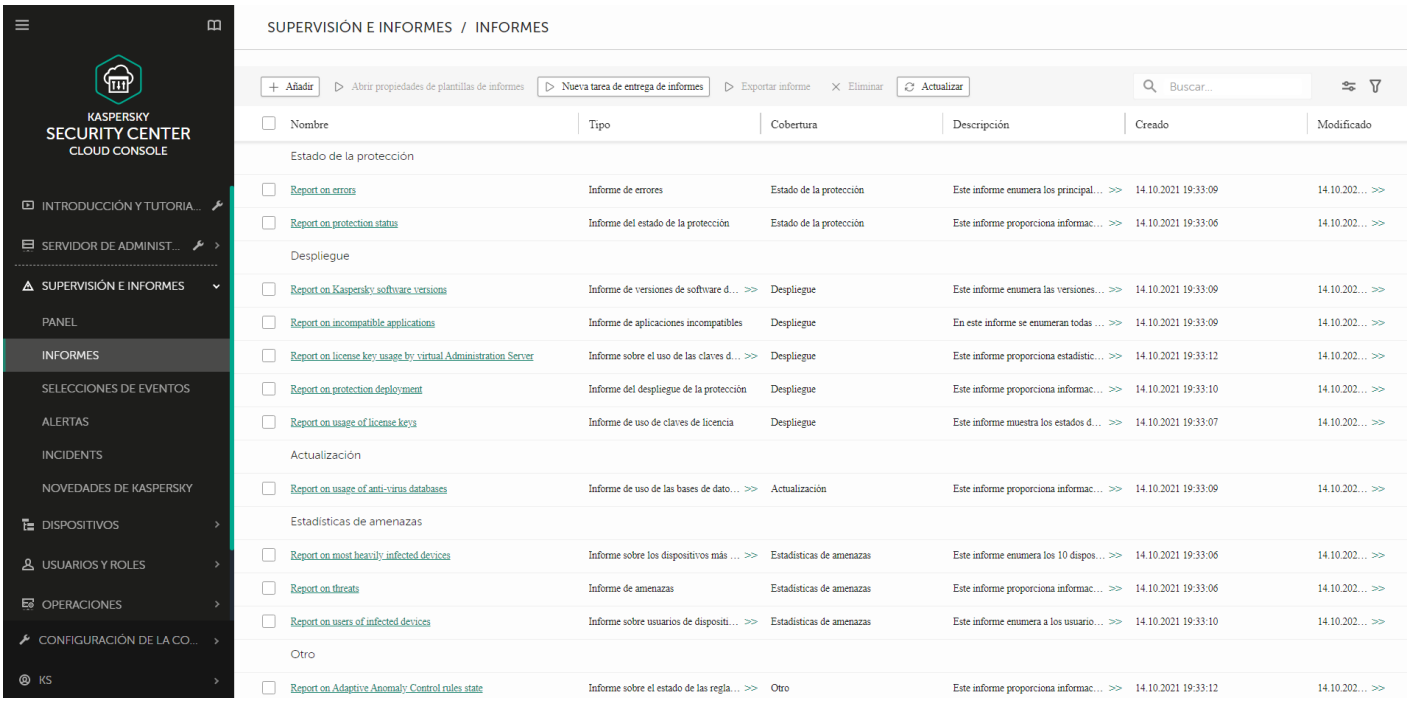
El panel brinda información gráfica que ayuda a controlar las tendencias de seguridad que se presentan en la red de la organización. (Vea la figura a continuación).



La sección 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 el envío de informes por correo electrónico (consulte la figura a continuación).



La sección 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**). También es posible crear selecciones de eventos personalizadas.

Notificaciones por correo electrónico

Puede configurar el envío de notificaciones por correo electrónico para mantenerse al tanto de los eventos que ocurren en Kaspersky Security Center Cloud Console y en los dispositivos de sus clientes.

Cómo trabajar con Kaspersky Security Center Cloud Console en un entorno de nube

En esta sección, se brinda información sobre las funciones de Kaspersky Security Center Cloud Console relacionadas con el uso y el mantenimiento de Kaspersky Security Center Cloud Console en un entorno de nube, como Amazon Web Services, Microsoft Azure o Google Cloud.

Para operar en un entorno de nube, se necesita una licencia especial. Si no cuenta con esta licencia, no podrá interactuar con los elementos de interfaz vinculados a los dispositivos de nube.

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

Opciones de licencia en un entorno de nube

Puede trabajar en un entorno de nube tanto en el modo de prueba como en el modo comercial de Kaspersky Security Center Cloud Console:

- El modo de prueba brinda acceso a todas las funciones para entornos de nube a lo largo de todo el período de validez del espacio de trabajo. No se requiere una licencia.
- En modo comercial, tendrá acceso a las funciones para entornos de nube solo si ha agregado una clave de licencia de Kaspersky Hybrid Cloud Security como clave activa en las propiedades del Servidor de administración.

En ambos casos, la característica Administración de vulnerabilidades y parches se activará 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.

Preparativos para trabajar en un entorno de nube a través de Kaspersky Security Center Cloud Console

En esta sección, aprenderá a prepararse para trabajar con Kaspersky Security Center Cloud Console en los siguientes entornos de nube:

- Amazon Web Services
- Microsoft Azure
- Google Cloud

Trabajar en el entorno de nube de Amazon Web Services

En esta sección, aprenderá a 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 eran válidas al momento de la publicación de Kaspersky Security Center Cloud Console.

Acerca del trabajo con el entorno de nube de Amazon Web Services

Para operar 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 eran válidas al momento de la publicación de Kaspersky Security Center Cloud Console.

Creación de cuentas de usuario de IAM para instancias de Amazon EC2

En esta sección se describen las acciones que debe llevar a cabo para garantizar el correcto funcionamiento de Kaspersky Security Center Cloud Console. Algunas de las acciones suponen operar 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.

Comprobar que Kaspersky Security Center Cloud Console tenga los permisos para trabajar con AWS

Para operar en el entorno de nube de Amazon Web Services utilizando Kaspersky Security Center Cloud Console, debe crear una *cuenta de usuario de IAM*, que Kaspersky Security Center Cloud Console utilizará para interactuar 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*).

Para crear la cuenta de usuario de IAM, utilice 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.

Creación de una cuenta de usuario de IAM para trabajar con Kaspersky Security Center Cloud Console

Para trabajar con Kaspersky Security Center Cloud Console, necesitará una cuenta de usuario de IAM. Puede crear una cuenta de usuario de IAM con todos los permisos necesarios o, si lo prefiere, puede crear dos cuentas de usuario separadas.

Se creará automáticamente para el usuario de IAM una *clave de acceso de IAM*, que usted deberá proporcionar a Kaspersky Security Center 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 agregar el permiso, revíselo para asegurarse de que todo sea correcto. 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 eran válidas al momento de la publicación de Kaspersky Security Center Cloud Console.

Trabajar en el entorno de nube de Microsoft Azure

Esta sección proporciona información que le servirá para operar y mantener Kaspersky Security Center Cloud Console en un entorno de nube proporcionado por Microsoft Azure. Encontrará también detalles sobre el despliegue de la protección en las máquinas virtuales de este entorno de nube.

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 en Azure con los permisos necesarios para instalar 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, un id. de aplicación de Azure y la contraseña de la aplicación en Azure. Si ya tiene una suscripción, puede utilizarla.

Una suscripción de Azure otorga a su titular acceso al Portal de administración de la plataforma Microsoft Azure y a los servicios de Microsoft Azure. El titular puede usar la plataforma Microsoft Azure para administrar servicios como Azure SQL y Azure Storage.

Para crear una suscripción de Microsoft Azure,

Vaya a https://learn.microsoft.com/es-mx/azure/cost-management-billing/manage/create-subscription y siga las instrucciones que allí se indican.

Encontrará más detalles sobre la creación de una suscripción en el sitio web de Microsoft website. Se le brindará un id. de suscripción, que luego cargará en Kaspersky Security Center Cloud Console junto con el id. de 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 eran válidas al momento de la publicación 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 desea no solo detectar máquinas virtuales, sino también desplegar la protección mediante la API de Azure, el id. de la aplicación en Azure deberá tener la función Colaborador de máquina virtual.

Siga las instrucciones del sitio web de Microsoft para asignar una función al id. de la aplicación en Azure.

Trabajar con Google Cloud

En esta sección, encontrará información para operar con Kaspersky Security Center Cloud Console en un entorno de nube provisto 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 para entornos de nube de Kaspersky Security Center Cloud Console

Para configurar Kaspersky Security Center Cloud Console a través de este asistente, debe tener lo siguiente:

- Las credenciales específicas de un entorno de nube:
  - Una cuenta de usuario de IAM a la que se le haya otorgado el derecho de sondear el segmento de la nube (para operar con Amazon Web Services)
  - Id. de aplicación, contraseña y suscripción de Azure (para operar con Microsoft Azure)
  - Correo electrónico del cliente, id. de proyecto y clave privada de Google (para operar con Google Cloud)
- Paquetes de instalación:
  - Agente de red para Windows

- Agente de red para Linux
- Kaspersky Endpoint Security for Linux

- Complemento web para Kaspersky Endpoint Security for Linux
- Al menos uno de los siguientes:
  - Paquete de instalación y complemento web para Kaspersky Endpoint Security para Windows (recomendado)
  - Paquete de instalación y complemento de administración de Kaspersky Security for Windows Server

Si utilizó una licencia de Kaspersky Hybrid Cloud Security para crear su espacio de trabajo, el Asistente de configuración para entornos de nube se iniciará automáticamente cuando se conecte a Kaspersky Security Center Cloud Console por primera vez. De ser necesario, podrá volver a abrir el Asistente de configuración para entornos de nube en cualquier otro momento.

Para iniciar el Asistente de configuración para entornos de nube manualmente:

En el menú principal, vaya a **Descubrimiento y despliegue → Despliegue y asignación → Configurar entorno de nube**.

Se inicia el asistente.

Necesitará aproximadamente quince minutos para completar los pasos del asistente.

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

Solo se mostrará este paso si utilizó una licencia que no sea la de Kaspersky Hybrid Cloud Security al crear el espacio de trabajo y si nunca agregó la clave de licencia de este producto en el campo de activación del Servidor de administración. Si ese fuera el 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 va a realizar el despliegue de Kaspersky Security Center Cloud Console: AWS, Azure o Google Cloud.

  Si planea trabajar con más de un entorno de nube, seleccione uno en este momento y vuelva a ejecutar el asistente más tarde.

- **Nombre de conexión**

  Escriba un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres Unicode.

  El nombre que escriba aquí será también el nombre del grupo de administración para los dispositivos de nube.

  Si planea trabajar con más de un entorno de nube, sugerimos que incluya el nombre del entorno en el nombre de la conexión (por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google").

Introduzca las credenciales para autorizarse en el entorno de nube seleccionado.

AWS

Si selecciona AWS como tipo de segmento de la nube, use una clave de acceso de AWS IAM para permitir el sondeo del segmento. Ingrese los siguientes datos de la 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.

Este campo estará disponible una vez que seleccione 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.

  Este campo estará disponible una vez que seleccione 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 aplicación de Azure**

  Usted creó el id. de la aplicación en el portal de Azure.

  No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

- **Id. de suscripción de Azure**

  Creó esta suscripción en el portal de Azure.

- **Contraseña de la aplicación en Azure**

  Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

  Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

  Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

- **Nombre de la cuenta de almacenamiento de Azure**

  Usted creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center Cloud Console.

- **Clave de acceso al almacenamiento de Azure**

Recibió una contraseña (o clave) cuando creó la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center Cloud Console.

La clave está disponible en la sección "Overview of the Azure storage account" ("Descripción general de la cuenta de almacenamiento de Azure"), subsección "Keys" ("Claves").

Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

Google Cloud

Si ha seleccionado Google Cloud como tipo de segmento de nube, debe introducir los siguientes datos para permitir el sondeo del segmento:

- **Correo electrónico del cliente**

  La dirección de correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. de proyecto**

  El id. que le enviaron cuando registró su proyecto en Google Cloud.

- **Clave privada**

  La secuencia de caracteres que le enviaron como clave privada cuando registró su proyecto en Google Cloud. Recomendamos que copie y pegue esta secuencia para evitar errores.

  Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

La aplicación guarda la conexión configurada.

El Asistente de configuración para entornos de nube permite configurar los ajustes de un único segmento. Si necesita administrar otros segmentos de nube, podrá agregar las conexiones necesarias en otro momento.

Haga clic en **Siguiente** para continuar.

Paso 4. Sondeo del segmento y configuración de la sincronización con la nube

En este paso, la aplicación comienza a sondear el segmento de la nube. También crea automáticamente un grupo de administración especial para los dispositivos de nube. Los dispositivos que se detecten durante el sondeo se agregarán a este nuevo grupo. De manera predeterminada, el proceso de sondeo del segmento de la nube se repetirá cada 5 minutos (puede cambiar este valor más adelante).

La aplicación también creará una regla de movimiento automático llamada **Sincronizar con la nube**. Los dispositivos virtuales que se detecten en los subsiguientes sondeos de la red de la nube se moverán a un subgrupo correspondiente dentro del grupo **Dispositivos administrados\Cloud**.

Defina un valor para la opción **Sincronizar los grupos de administración con la estructura de nube**.

Si habilita está opción, se creará el grupo **Cloud** automáticamente dentro el grupo **Dispositivos administrados** y se iniciará un proceso para descubrir dispositivos en la nube. Las instancias y las máquinas virtuales que se detecten cada vez que se sondee la red de la nube se agregarán al grupo "Cloud". La estructura de subgrupos de administración dentro de este grupo se hará coincidir con la estructura del segmento de la nube (en AWS, las zonas de disponibilidad y los grupos de ubicación no estarán representados en la estructura; en Azure, no estarán representadas las subredes). Los dispositivos que no se hayan identificado como instancias en el entorno de nube estarán en el grupo **Dispositivos no asignados**. La estructura de grupos le permitirá usar tareas de instalación grupales para instalar aplicaciones antivirus en las instancias, así como definir directivas diferentes para grupos diferentes.

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 la nube** y aplicarla. Al aplicar la regla, la estructura de subgrupos del grupo "Cloud" se hará coincidir con la estructura del segmento de la nube.

Esta opción está deshabilitada de forma predeterminada.

Haga clic en **Siguiente** para continuar.

Paso 5. Seleccionar una aplicación para crear una directiva y tareas

Este paso solo se muestra si tiene paquetes de instalación y complementos para Kaspersky Endpoint Security para Windows y Kaspersky Security for Windows Server. Si tiene un complemento y un paquete de instalación solo para una de esas aplicaciones, este paso se omite y Kaspersky Security Center Cloud Console crea una directiva y tareas para la aplicación existente.

Seleccione una aplicación para la que desea crear una directiva.

- Kaspersky Endpoint Security para Windows
- Kaspersky Security for Windows Server

Paso 6. Configuración de Kaspersky Security Network para Kaspersky Security Center Cloud Console

No verá este paso si está utilizando Kaspersky Security Center Cloud Console en modo de prueba o en un Servidor de administración virtual.

Configure las opciones que controlan la transmisión de datos 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 utilizar Kaspersky Security Network**

Kaspersky Security Center Cloud Console y las aplicaciones administradas de los dispositivos cliente transferirán información sobre sus operaciones a Kaspersky Security Network de manera automática. Participar en Kaspersky Security Network permite que las bases de datos con información sobre virus y otros riesgos se actualicen más rápidamente, lo cual se traduce en una mayor velocidad de respuesta ante amenazas a la seguridad emergentes.

- **No acepto utilizar Kaspersky Security Network**

  Kaspersky Security Center 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 opta por no participar en Kaspersky Security Network, estas aplicaciones no enviarán información a Kaspersky. Si cambia de opinión en algún momento, podrá indicarlo a través de la directiva de la aplicación.

Haga clic en **Siguiente** para continuar.

Paso 7. Creación de una configuración de protección inicial

Puede ver la lista de directivas y tareas creadas.

Espere a que finalice la creación de las tareas y directivas. A continuación, haga clic en **Siguiente**. En la última página del asistente, haga clic en el botón **Finalizar** para salir.

Sondeo de segmentos de red con Kaspersky Security Center Cloud Console

La información disponible sobre la estructura de la red (y sobre los dispositivos que la componen) deriva de sondear los segmentos de nube en forma periódica a través de las herramientas que brindan las API de AWS, Azure y Google. Kaspersky Security Center Cloud Console usa la información que se recaba de esta manera 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 nube, necesitará contar con ciertos derechos, que pueden otorgarse a través de una cuenta de usuario de IAM (en el caso de AWS), con un id. de aplicación y la contraseña de esa aplicación (en el caso de Azure) o con un id. de proyecto, una clave privada y el correo electrónico del cliente (en el caso de Google Cloud).

Puede agregar y eliminar conexiones para cada segmento de nube y definir una programación de sondeo para cada segmento.

Agregar conexiones para sondear segmentos de 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 **Descubrimiento y despliegue** → **Descubrimiento** → **Cloud**.
2. En la ventana que se abre, haga clic en **Propiedades**.
3. En la ventana **Configuración** que se abre, haga clic en **Agregar**.

   Se abre la ventana **Configuración del segmento de la nube**.
4. Escriba el nombre del entorno de nube correspondiente a la conexión que se usará para sondear el segmento de nube:

   - **Entorno de nube**

     Seleccione el entorno de nube en el que va a realizar el despliegue de Kaspersky Security Center Cloud Console: AWS, Azure o Google Cloud.

     Si planea trabajar con más de un entorno de nube, seleccione uno en este momento y vuelva a ejecutar el asistente más tarde.

   - **Nombre de conexión**

     Escriba un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres Unicode.

     El nombre que escriba aquí será también el nombre del grupo de administración para los dispositivos de nube.

     Si planea trabajar con más de un entorno de nube, sugerimos que incluya el nombre del entorno en el nombre de la conexión (por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google").
5. Introduzca las credenciales para autorizarse en el entorno de nube seleccionado.

   - Si seleccionó AWS, configure los siguientes ajustes:

     - **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.

       Este campo estará disponible una vez que seleccione 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.

Este campo estará disponible una vez que seleccione 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 de Azure**

    Usted creó el id. de la aplicación en el portal de Azure.

    No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

  - **Id. de suscripción de Azure**

    Creó esta suscripción en el portal de Azure.

  - **Contraseña de la aplicación en Azure**

    Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

    Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

    Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

  - **Nombre de la cuenta de almacenamiento de Azure**

    Usted creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center Cloud Console.

  - **Clave de acceso al almacenamiento de Azure**

    Recibió una contraseña (o clave) cuando creó la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center Cloud Console.

    La clave está disponible en la sección "Overview of the Azure storage account" ("Descripción general de la cuenta de almacenamiento de Azure"), subsección "Keys" ("Claves").

    Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

Si seleccionó Google Cloud, configure los siguientes ajustes:

- **Correo electrónico del cliente**

La dirección de correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. de proyecto**

  El id. que le enviaron cuando registró su proyecto en Google Cloud.

- **Clave privada**

  La secuencia de caracteres que le enviaron como clave privada cuando registró su proyecto en Google Cloud. Recomendamos que copie y pegue esta secuencia para evitar errores.

  Para ver los caracteres que ha escrito, haga clic en el botón **Mostrar** y manténgalo presionado.

6. Si lo desea, haga clic en **Establecer programación de sondeo** y cambie la configuración predeterminada.

La conexión se guarda en la configuración de la aplicación.

Una vez que el nuevo segmento de la nube se haya sondeado por primera vez, el subgrupo correspondiente a ese segmento aparecerá en el grupo de administración **Dispositivos administrados\Nube**.

Si las credenciales que introdujo no son correctas, no se encontrará ninguna instancia durante el sondeo del segmento y, en consecuencia, no aparecerá ningún subgrupo nuevo en el grupo de administración **Dispositivos administrados\Cloud**.

Eliminar conexiones para el sondeo de segmentos de nube

Si ya no necesita que la aplicación sondee un segmento de nube en particular, puede eliminar la conexión correspondiente a ese segmento de la lista de conexiones disponibles. Lo mismo puede hacer si, por ejemplo, los permisos para sondear el segmento se han transferido a un usuario que utiliza otras credenciales.

Para eliminar una conexión:

1. En el menú principal, vaya a **Descubrimiento y despliegue** → **Descubrimiento** → **Cloud**.
2. En la ventana que se abre, haga clic en **Propiedades**.
3. En la ventana **Configuración** que se abre, haga clic en el nombre del segmento que desee eliminar.
4. Haga clic en **Eliminar**.
5. En la ventana que se abre, haga clic en el botón **Aceptar** para confirmar su elección.

La conexión se eliminará. Los dispositivos del segmento de nube asociado a la conexión se eliminarán automáticamente de los grupos de administración.

Configurar la programación de sondeo con 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.

De manera predeterminada, el Asistente de configuración para entornos de nube fija la frecuencia de sondeo en cinco minutos. Puede cambiar este valor en cualquier momento y definir una programación diferente. No se recomienda configurar una frecuencia de sondeo inferior a cinco minutos: podría provocar inconvenientes en el funcionamiento de la API.

Para configurar la programación de sondeo para un segmento de nube:

1. En el menú principal, vaya a **Descubrimiento y despliegue** → **Descubrimiento** → **Cloud**.
2. En la ventana que se abre, haga clic en **Propiedades**.
3. En la ventana **Configuración** que se abre, haga clic en el nombre del segmento para el que quiera configurar la programación de sondeo.

   Se abre la ventana **Configuración del segmento de la nube**.
4. En la ventana **Configuración del segmento de la nube**, haga clic en **Establecer programación de sondeo**.

   Se abre la ventana **Programación**.
5. En la ventana **Programación**, configure los siguientes ajustes:

   - **Inicio programado**

     Opciones de programación para el sondeo:

     - Cada N días

       Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la fecha y hora indicadas. Cada sondeo estará separado del anterior por el número de días que indique.

       De forma predeterminada, se realizará un sondeo todos los días, a partir de la fecha y hora actuales del sistema.

     - Cada N minutos

       Se realizará un sondeo en forma periódica, a intervalos regulares, a partir de la hora indicada. Cada sondeo estará separado del anterior por el número de minutos que indique.

       De forma predeterminada, se realizará un sondeo cada cinco minutos, a partir de la hora actual del sistema.

     - Por días de la semana

       Se realizará un sondeo en forma periódica, a intervalos regulares, en el día de la semana y a la hora que indique.

       De manera predeterminada, el sondeo se ejecutará todos los viernes a las 18:00:00.

- **Cada mes en los días especificados de semanas seleccionadas**

  Se realizará un sondeo en forma periódica, a intervalos regulares, en los días del mes y a la hora que indique.

  Por defecto, no hay ningún día seleccionado; la hora de inicio predeterminada es las 18:00:00 p. m.

- **Intervalo entre inicios (días)**

  Indique a cuántos días o minutos, según el caso, equivale N.

- **Primera ejecución**

  Indique cuándo se realizará el primer sondeo.

- **Ejecutar tareas no realizadas**

  Si su espacio de trabajo no está disponible en el momento en que se debe realizar un sondeo, Kaspersky Security Center Cloud Console puede realizar ese sondeo en cuanto el espacio de trabajo vuelve a estar disponible o puede esperar a que llegue el turno del siguiente sondeo programado.

  Si esta opción está habilitada, Kaspersky Security Center Cloud Console iniciará el sondeo en cuanto el espacio de trabajo vuelva a estar disponible

  Si esta opción está deshabilitada, Kaspersky Security Center Cloud Console esperará a que llegue el turno del siguiente sondeo programado.

  Esta opción está activada de forma 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 de segmentos de nube en 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 **Descubrimiento y despliegue** → **Descubrimiento** → **Cloud**.

Se muestran los segmentos de nube que se pueden sondear.

Ver las propiedades de los dispositivos de nube en 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 dispositivos de 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 dispositivos de Azure, se muestran las siguientes propiedades:

   - **Dispositivo encontrado mediante API** (valor: **Microsoft Azure**)
   - **Región en la nube**
   - **Subred de nube**

   Para dispositivos de 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

El Asistente de configuración para entornos de nube crea una regla llamada "Sincronizar con la nube" de manera automática. Esta regla permite mover automáticamente los dispositivos detectados en cada sondeo del grupo "Dispositivos no asignados" al grupo "Dispositivos administrados\Cloud" para poder administrarlos en forma centralizada. De manera predeterminada, una vez que se crea esta regla, se la deja habilitada. Puede deshabilitar, modificar o aplicar la regla en cualquier momento.

Para aplicar la regla "Sincronizar con la nube" o modificar sus propiedades:

1. En el menú principal, vaya a **Descubrimiento y despliegue → Despliegue y asignación → Reglas de movimiento**.

   Se abre una lista de reglas de movimiento.

2. En la lista de reglas de movimiento, seleccione **Sincronizar con la nube**.

   Se abre la ventana de propiedades de la regla.

3. De ser necesario, configure los siguientes ajustes en la pestaña **Segmentos de nube** de la pestaña **Condiciones de la regla**:

   - **El dispositivo se encuentra en un segmento de la nube**

     La regla solo se aplicará a los dispositivos que se encuentren en el segmento de nube seleccionado. De lo contrario, la regla se aplicará a todos los dispositivos que hayan sido detectados.

     Esta opción está seleccionada de forma predeterminada.

   - **Incluir objetos secundarios**

     La regla se aplicará a todos los dispositivos del segmento seleccionado y a todas las subsecciones de nube anidadas. De lo contrario, la regla solo se aplicará a los dispositivos que estén en el segmento raíz.

     Esta opción está seleccionada de forma predeterminada.

   - **Mover los dispositivos de objetos anidados a subgrupos correspondientes**

     Si esta opción está habilitada, los dispositivos de los objetos anidados se moverán automáticamente a los subgrupos que se correspondan con su estructura.

     Si esta opción está deshabilitada, los dispositivos de los objetos anidados se moverán automáticamente a la raíz del subgrupo "Cloud" y no habrá más ramificaciones.

     Esta opción está activada de forma predeterminada.

   - **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados**

     Si esta opción está habilitada, cuando la estructura del grupo **Dispositivos administrados\Cloud** no tenga subgrupos que coincidan con la sección en la que esté incluido un dispositivo, Kaspersky Security Center Cloud Console creará los subgrupos necesarios. Por ejemplo, si se detecta una nueva subred durante el descubrimiento de dispositivos, se creará un nuevo grupo con el mismo nombre en el grupo **Dispositivos administrados\Cloud**.

     Si esta opción está deshabilitada, Kaspersky Security Center Cloud Console no creará nuevos subgrupos. Si se descubre una nueva subred al sondear la red, por ejemplo, no se creará un nuevo grupo con el mismo nombre en el grupo **Dispositivos administrados\Cloud**, y los dispositivos que se encuentren en la subred detectada se moverán al grupo **Dispositivos administrados\Cloud**.

     Esta opción está activada de forma predeterminada.

- Eliminar subgrupos para los que no se encuentre coincidencia en los segmentos de nube

  Si esta opción está habilitada, la aplicación eliminará del grupo "Cloud" todo subgrupo que no tenga contraparte en un objeto de nube existente.

  Si esta opción está deshabilitada, se conservarán los subgrupos que no tengan contraparte en un objeto de nube existente.

  Esta opción está activada de forma predeterminada.

Si habilitó la opción **Sincronizar los grupos de administración con la estructura de nube** al utilizar el Asistente de configuración para entornos de nube, la regla **Sincronizar con la nube** ya tendrá habilitadas las opciones **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados** y **Eliminar subgrupos para los que no se encuentre coincidencia en los segmentos de nube**.

Si no habilitó la opción **Sincronizar los grupos de administración con la estructura de nube**, la regla **Sincronizar con la nube** no tendrá estas opciones habilitadas. Si, por el modo en que usted utiliza Kaspersky Security Center Cloud Console, necesita que la estructura de subgrupos dentro del subgrupo **Dispositivos administrados\Cloud** coincida con la estructura de los segmentos de nube, habilite las opciones **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados** y **Eliminar subgrupos para los que no se encuentre coincidencia en los segmentos de nube** en las propiedades de la regla y aplique la regla.

4. En la lista desplegable **Dispositivo encontrado mediante API**, seleccione uno de los siguientes valores:

   - **No**. El dispositivo no se puede detectar con la API de AWS, Azure o Google (o bien el dispositivo no se encuentra en el entorno de nube, o sí está en el entorno de nube, pero, por algún motivo, no se lo puede detectar con 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 mediante la API de Google, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Google.
   - Ningún valor. Este criterio no se puede aplicar.

5. Si es necesario, configure las propiedades de la regla en las demás secciones.

La regla de movimiento queda configurada.

Instalación remota de aplicaciones en máquinas virtuales de Azure

Para instalar aplicaciones en máquinas virtuales de Microsoft Azure, debe tener una licencia válida.

Kaspersky Security Center Cloud Console admite los siguientes escenarios:

- El dispositivo cliente se descubre a través de la API de Azure y la instalación se realiza, también, a través de una API. El uso de la API de Azure significa que solo puede instalar las siguientes aplicaciones:
  - Kaspersky Endpoint Security for Linux

- Kaspersky Endpoint Security para Windows
- Kaspersky Security for Windows Server

- El dispositivo cliente se descubre a través de la API de Azure y la instalación se realiza a través de un punto de distribución o, si no hay puntos de distribución disponibles, de manera manual, utilizando paquetes de instalación independientes. Este método sirve para instalar cualquier aplicación compatible con Kaspersky Security Center Cloud Console.

Para instalar una aplicación de forma remota en una máquina virtual de Azure, cree una tarea de este modo:

1. En el menú principal, vaya a **Activos (dispositivos)** → **Tareas**.
2. Haga clic en **Agregar**.

   Se inicia el Asistente para crear nueva tarea.
3. Siga las instrucciones del asistente:

   a. Seleccione **Instalar aplicación de forma remota** como tipo de tarea.

   b. En la página **Paquetes de instalación**, seleccione **Instalación remota mediante Microsoft Azure API**.

   c. Al momento de seleccionar la cuenta con la que se accederá a los dispositivos, use una cuenta de Azure existente o haga clic en **Agregar** e ingrese las credenciales de su cuenta de Azure:

   - **Nombre de la cuenta de Azure**

     Escriba un nombre cualquiera para las credenciales que está introduciendo. El nombre aparecerá en la lista de cuentas para ejecutar la tarea.

   - **ID de aplicación de Azure**

     Usted creó el id. de la aplicación en el portal de Azure.

     No puede especificar más de un id. de aplicación de Azure para realizar sondeos u otros fines. Si desea sondear otro segmento de Azure, elimine primero la conexión de Azure existente.

   - **Contraseña de la aplicación en Azure**

     Recibió la contraseña correspondiente al id. de aplicación cuando creó dicho id.

     Los caracteres de la contraseña se muestran como asteriscos. Cuando empiece a introducir la contraseña, aparecerá el botón **Mostrar**. Haga clic en este botón y manténgalo presionado para ver los caracteres introducidos.

   d. Seleccione los dispositivos pertinentes en el grupo **Dispositivos administrados\Cloud**.

Cuando finalice el asistente, encontrará la tarea para instalar la aplicación en forma remota dentro de la lista de tareas.

Contacto con el servicio de soporte técnico

En esta sección se explica cómo obtener soporte técnico y se describen los términos que rigen este servicio.

Cómo obtener soporte técnico

Si no encuentra una solución a su problema en la documentación de Kaspersky Security Center Cloud Console o en alguna de las fuentes de información sobre Kaspersky Security Center Cloud Console, comuníquese con el servicio de soporte técnico de Kaspersky. Los especialistas del servicio de soporte técnico responderán a todas sus preguntas acerca de la instalación y el uso de Kaspersky Security Center 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.

Para comunicarse con el servicio de soporte técnico, puede elegir alguna de estas opciones:

- Puede visitar el sitio web del Soporte técnico
- Puede enviar una solicitud al servicio de soporte técnico a través del portal Kaspersky CompanyAccount

Consultas mediante Kaspersky CompanyAccount al servicio de soporte técnico

Kaspersky CompanyAccount es un portal para empresas que usan aplicaciones de Kaspersky. El portal Kaspersky CompanyAccount está diseñado para que los usuarios puedan comunicarse con los especialistas de Kaspersky fácilmente a través de solicitudes en línea. Puede usar Kaspersky CompanyAccount para seguir el estado de sus solicitudes en línea y también para almacenar un historial de solicitudes.

Puede registrar a todos los empleados de su organización bajo una única cuenta de Kaspersky CompanyAccount. Una cuenta única le permite administrar de forma centralizada las solicitudes electrónicas enviadas a Kaspersky por los empleados registrados y administrar los privilegios de esos empleados a través de Kaspersky CompanyAccount.

El portal Kaspersky CompanyAccount está disponible en los siguientes idiomas:

- Inglés
- Español
- Italiano
- Alemán
- Polaco
- Portugués
- Ruso

- Francés
- Japonés

Para obtener más información sobre Kaspersky CompanyAccount, visite el sitio web del servicio de soporte técnico.

Información necesaria para los especialistas del Soporte técnico de Kaspersky

Cuando se comunique 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 de espacio de trabajo
- Información de licencia
- Cantidad de aplicaciones instaladas
- ID y estado del inquilino

Puede encontrar esta información en la sección **Menú de su cuenta** → **Servicio de soporte técnico**. Copie y comparta esta información para obtener ayuda con su problema.

Fuentes de información acerca de la aplicación

La página de Kaspersky Security Center Cloud Console en el sitio web de Kaspersky

En la página de Kaspersky Security Center Cloud Console disponible en el sitio web de Kaspersky, encontrará información general sobre la aplicación, sus funciones y sus características.

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 disponible en la Base de conocimientos, encontrará artículos con información útil, recomendaciones y respuestas a las preguntas más frecuentes sobre cómo comprar, instalar y utilizar la aplicación.

Los artículos de la Base de conocimientos pueden resolver inquietudes relacionadas tanto con Kaspersky Security Center Cloud Console como con otras aplicaciones de Kaspersky. Los artículos de la Base de conocimientos también pueden contener noticias del Servicio de soporte técnico.

Discutir las aplicaciones de Kaspersky con la comunidad

Si su pregunta no requiere una respuesta inmediata, puede analizarla con los expertos de Kaspersky y con otros usuarios en nuestro foro.

Dentro del foro, puede ver temas de discusión existentes, publicar comentarios y crear nuevos temas de discusión.

> Se requiere una conexión a Internet para acceder a los recursos web.

Si no encuentra solución a su problema, comuníquese con el servicio de soporte técnico.

Problemas conocidos

Kaspersky Security Center 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 habilitado.

- En la directiva de Kaspersky Endpoint Security for Mac, si habilita la integración con KATA y no especifica la dirección del servidor y el certificado, un intento de habilitar 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 habilita la opción **Seleccionar dispositivos a los que se asignará la tarea**. Estas tareas no se pueden asignar a una selección de dispositivos o a dispositivos específicos. Si asigna la tarea *Descargar actualizaciones a los repositorios de puntos de distribución* o *Verificación de actualizaciones* a dispositivos específicos, la tarea se importará incorrectamente.

- Una vez que se completa la tarea de *Análisis de inventario* para un dispositivo Linux, al intentar enviar los archivos recibidos a Kaspersky para su análisis se produce un error.

- Cuando se intenta iniciar sesión en Kaspersky Security Center Cloud Console a través de los Servicios de federación de Active Directory (AD FS), pero no se tienen los permisos necesarios, Kaspersky Security Center Cloud Console aún muestra el error "Credenciales no válidas" en lugar de advertir sobre los permisos faltantes.

- La tarea "Administrar dispositivos" no funciona correctamente para dispositivos con 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 la vulnerabilidad en los 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. Bajo este rótulo se incluyen las actualizaciones críticas acumuladas a lo largo de un período de tiempo.

Administración centralizada de aplicaciones

Administración remota de aplicaciones a través de los servicios de administración que ofrece 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 el funcionamiento de las aplicaciones a través del sistema de administración remota y centralizada 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

Componente de Kaspersky Security Center Cloud Console que permite la interacción entre el Servidor de administración y las aplicaciones de Kaspersky instaladas en un nodo de red específico (estación de trabajo o servidor). Este componente es el mismo para todas las aplicaciones para Microsoft® Windows® de la empresa. Existen versiones independientes del Agente de red para las aplicaciones de Kaspersky desarrolladas para macOS y sistemas operativos de tipo Unix.

Aplicación incompatible

Aplicación antivirus que no fue creada por Kaspersky o aplicación de Kaspersky que no se puede administrar a través de Kaspersky Security Center 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 que contienen información sobre las amenazas a la seguridad informática de las que Kaspersky tiene conocimiento a la fecha de publicarse esas bases de datos. Las entradas de las bases de datos antivirus permiten detectar código malicioso en los objetos analizados. Las bases de datos antivirus son generadas por los especialistas de Kaspersky. Se actualizan cada una hora.

Brote de virus

Serie de intentos deliberados de infectar un dispositivo con un virus.

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 administrar el software de Kaspersky de manera remota 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 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.

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

Un equipo con un Agente de red instalado o un dispositivo móvil con una aplicación de seguridad de Kaspersky instalada.

Dispositivo con protección de UEFI

Dispositivo que cuenta con una solución o aplicación de Kaspersky para UEFI integrado en el nivel de la BIOS. La protección integrada garantiza que el dispositivo está protegido desde el momento en que se lo enciende. La protección en dispositivos sin software integrado, por el contrario, no comienza a funcionar sino hasta que la aplicación de seguridad se inicia.

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 necesitan 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

Un rótulo para aplicaciones de terceros que puede utilizarse para agrupar o encontrar aplicaciones. Asignada a una serie de aplicaciones, una etiqueta puede servir de condición para crear una selección de dispositivos.

Etiqueta de dispositivo

Un rótulo que se asigna a los dispositivos y que permite agruparlos, describirlos o encontrarlos.

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
- Error funcional
- Advertencia
- Información

Dos eventos de un mismo tipo pueden tener niveles de gravedad diferentes si ocurren en situaciones diferentes.

Grupo de administración

Un conjunto de dispositivos combinados de acuerdo con las funciones que realizan y con las aplicaciones de Kaspersky que tienen instaladas. Los dispositivos se agrupan y se tratan como una sola entidad para facilitar su administración. Cada grupo puede incluir otros grupos. Pueden crearse directivas de grupo y tareas de grupo para cada aplicación instalada en un grupo.

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 las aplicaciones de Kaspersky mediante los servicios proporcionados 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)

La interfaz de programación de aplicaciones de la plataforma AWS que utiliza Kaspersky Security Center Cloud Console. Las herramientas que provee la API de AWS se utilizan, específicamente, para sondear los 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 ejecutar tareas de administración y mantenimiento básicas en la red de una organización de forma centralizada. Kaspersky Next Expert View es una aplicación alojada y mantenida por Kaspersky. 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)

Una infraestructura de servicios en la nube que proporciona acceso a la base de datos de Kaspersky con información constantemente actualizada sobre la reputación de los archivos, recursos web y software. Kaspersky Security Network permite que las aplicaciones de Kaspersky respondan más rápido a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de enfrentar falsos positivos.

Nagent ligero (LWNGT)

Protocolo para la interacción con Kaspersky Endpoint Security en dispositivos móviles. El LWNGT (también llamado protocolo móvil) funciona como Agente de red, pero sin instalar el Agente de red en dispositivos móviles.

Nivel de importancia del parche

Atributo del parche. Existen cinco niveles de importancia para los parches de Microsoft y los de terceros:

- Crítico
- Alto
- Medio
- Bajo
- Desconocido

El nivel de importancia de un parche de terceros o de Microsoft está determinado por el nivel de gravedad menos favorable entre las vulnerabilidades que el parche debe reparar.

Operador de Kaspersky Security Center Cloud Console

Usuario que supervisa el estado y el funcionamiento de un sistema de protección administrado mediante Kaspersky Security Center Cloud Console.

Paquete de instalación

Conjunto de archivos que se crea para instalar una aplicación de Kaspersky de manera remota, mediante el sistema de administración a distancia Kaspersky Security Center 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 nominado de los valores de configuración definidos en una directiva. Este subconjunto se distribuye en dispositivos de destino junto con la directiva y se complementa bajo una condición específica denominada Condición de activación del perfil.

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 en el que se ha instalado el Agente de red y que se utiliza para distribuir actualizaciones, realizar sondeos de red, instalar aplicaciones en forma remota y recopilar información sobre los equipos asociados a un grupo de administración o a un dominio de difusión. Es tarea del administrador determinar qué dispositivos actuarán como puntos de distribución y designarlos como tales manualmente.

Repositorio de eventos

Una parte de la base de datos del Servidor de administración dedicada al almacenamiento de información sobre los 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 centralmente información sobre las aplicaciones de Kaspersky instaladas en la red corporativa. También se lo puede usar para administrar estas 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 administrar el sistema de protección de la red de una organización cliente.

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

- Los servidores de administración virtuales solo pueden operar como servidores de administración secundarios.

- Los servidores de administración virtuales no admiten la creación de servidores de administración secundarios (sean o no 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.

Subred de reconocimiento de ubicación de red (NLA)

Servicio de Windows que ayuda al sistema operativo a identificar la red a la que está conectado. NLA detecta cambios en la red y ajusta la configuración de seguridad del dispositivo.

Tarea

Las funciones que realiza la aplicación de Kaspersky se implementan en forma de tareas. Algunas de estas tareas son Protección de archivos en tiempo real, Análisis completo del equipo y Actualización de las bases de datos.

Tarea de grupo

Tarea que se define para un grupo de administración y se ejecuta en todos los dispositivos cliente de ese grupo.

Tarea local

Una tarea definida y ejecutada en un solo equipo cliente.

Tarea para dispositivos específicos

Tarea asignada a un conjunto de dispositivos cliente tomados de grupos de administración arbitrarios y realizada en dichos dispositivos.

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

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

Encontrará información sobre el código de terceros en el archivo legal_notices.txt.

El archivo legal_notices.txt también se encuentra en la carpeta de instalación de Network Agent for Windows y Network Agent for Linux.

Para obtener información adicional sobre el código de terceros que se utiliza 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 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 o marcas comerciales registradas de Cloud Software Group, Inc. y/o sus filiales en los Estados Unidos y/u otros países.

Cloudflare, el logotipo de Cloudflare y Cloudflare Workers son marcas comerciales o marcas comerciales registradas de Cloudflare, Inc. en los Estados Unidos y otras jurisdicciones.

Corel y CorelDRAW son marcas comerciales o marcas comerciales registradas de Corel Corporation o sus filiales en Canadá, Estados Unidos 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 filiales en Estados Unidos y otros países.

BlackBerry es propiedad de Research In Motion Limited y está registrada en los Estados Unidos y puede estar pendiente o registrada en otros países.

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.