

kaspersky

Kaspersky Endpoint Security 10 Service Pack 2 para Windows

© 2022 AO Kaspersky Lab

Contenido

[Acerca de Kaspersky Endpoint Security 10 Service Pack 2 para Windows](#)

[Novedades](#)

[Kit de distribución](#)

[Organización de la protección del equipo](#)

[Requisitos de hardware y software](#)

[Instalación y eliminación de la aplicación](#)

[Instalación de la aplicación](#)

[Acerca de las formas de instalar la aplicación](#)

[Instalación de la aplicación mediante el Asistente de instalación](#)

[Paso 1. Asegúrese de que el equipo cumple con los requisitos de instalación](#)

[Paso 2. Página de bienvenida del proceso de instalación](#)

[Paso 3. Visualización del Contrato de licencia](#)

[Paso 4. Selección del tipo de instalación](#)

[Paso 5. Selección de los componentes de la aplicación que se van a instalar](#)

[Paso 6. Selección de la carpeta de destino](#)

[Paso 7. Adición de exclusiones de análisis de virus](#)

[Paso 8. Preparación de la instalación de la aplicación](#)

[Paso 9. Instalación de la aplicación](#)

[Instalación de la aplicación desde la línea de comandos](#)

[Instalando remotamente la aplicación usando System Center Configuration Manager](#)

[Descripción de la configuración de instalación del archivo setup.ini](#)

[Asistente de configuración inicial](#)

[Activación de la aplicación](#)

[Activar con un código de activación](#)

[Activar con un archivo clave](#)

[Selección de funciones que activar](#)

[Completar la activación](#)

[Análisis del sistema operativo](#)

[Finalización de la configuración inicial de la aplicación](#)

[Declaración de Kaspersky Security Network](#)

[Acerca de las formas de actualizar una versión antigua de la aplicación](#)

[Eliminación de la aplicación](#)

[Acerca de las formas de eliminar la aplicación](#)

[Eliminación de la aplicación mediante el Asistente de instalación](#)

[Paso 1. Almacenamiento de los datos de la aplicación para su uso posterior](#)

[Paso 2. Confirmación de la eliminación de la aplicación](#)

[Paso 3. Eliminación de la aplicación. Completando eliminación](#)

[Eliminación de la aplicación de la línea de comandos](#)

[Eliminar los objetos y datos que permanecen después de la operación de prueba del Agente de autenticación](#)

[Interfaz de la aplicación](#)

[Icono de la aplicación en el área de notificaciones de la barra de tareas](#)

[Menú contextual del icono de la aplicación](#)

[Ventana principal de la aplicación](#)

[Configurar pestaña Configuración de la aplicación](#)

[Pestaña Protección y control de aplicaciones](#)

[Licencias de la aplicación](#)

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

[Acerca de la licencia](#)

[Acerca del certificado de la licencia](#)

[Acerca de la suscripción](#)

[Acerca del código de activación](#)

[Acerca de la clave](#)

[Acerca del archivo llave](#)

[Acerca de la provisión de datos](#)

[Visualización de información de la licencia](#)

[Compra de una licencia](#)

[Renovación de licencias](#)

[Renovación de suscripciones](#)

[Consulta del sitio web del proveedor de servicios](#)

[Acerca de los métodos de activación de la aplicación](#)

[Uso del asistente de activación para activar la aplicación](#)

[Activación de la aplicación desde la línea de comandos](#)

[Inicio y detención de la aplicación](#)

[Activación y desactivación de la ejecución automática de la aplicación](#)

[Inicio y detención manuales de la aplicación](#)

[Suspensión y reanudación de la protección y el control del equipo](#)

[Protección del sistema de archivos del equipo. Antivirus de archivos](#)

[Acerca de Antivirus de archivos](#)

[Activación y desactivación del Antivirus de archivos](#)

[Suspensión automática del Antivirus de archivos](#)

[Configuración del Antivirus de archivos](#)

[Cambiar el nivel de seguridad](#)

[Modificación de la acción que Antivirus de archivos debe realizar en los archivos infectados](#)

[Edición de la cobertura de protección del Antivirus de archivos](#)

[Uso del Analizador heurístico con Antivirus de archivos](#)

[Uso de tecnologías de análisis en el funcionamiento de Antivirus de archivos](#)

[Optimización del análisis de archivos](#)

[Análisis de archivos compuestos](#)

[Modificación del modo de análisis](#)

[Protección del correo electrónico. Antivirus del correo](#)

[Acerca de Antivirus del correo](#)

[Activación y desactivación de Antivirus del correo](#)

[Configuración de Antivirus del correo](#)

[Modificación del nivel de seguridad del correo](#)

[Modificación de las acciones que se van a realizar en mensajes de correo electrónico infectados](#)

[Edición de la Cobertura de protección del Antivirus del correo](#)

[Analizar archivos compuestos adjuntos a mensajes de correo electrónico](#)

[Filtrar adjuntos de mensajes de correo electrónico](#)

[Análisis de correos electrónicos en Microsoft Office Outlook](#)

[Configurar el análisis del correo en Outlook](#)

[Configurar el análisis del correo utilizando Kaspersky Security Center](#)

[Protección del equipo en Internet. Antivirus Internet](#)

[Acerca de Antivirus Internet](#)

[Activación y desactivación del Antivirus Internet](#)

[Configuración de Antivirus Internet](#)

[Modificación del nivel de seguridad del tráfico web](#)

[Modificación de las acciones que se van a realizar en objetos maliciosos del tráfico web](#)

[Análisis de Antivirus Internet de direcciones URL con bases de datos de direcciones web fraudulentas y maliciosas](#)

[Uso del Analizador heurístico con Antivirus Internet](#)

[Modificación de la lista de direcciones URL de confianza](#)

[Protección del tráfico de clientes de MI. Antivirus para chat](#)

[Acerca de Antivirus para chat](#)

[Activación y desactivación del Antivirus para chat](#)

[Configuración de Antivirus para chat](#)

[Creación de la Cobertura de protección del Antivirus para chat](#)

[Análisis de direcciones URL con bases de datos de direcciones URL maliciosas y fraudulentas con Antivirus para chat](#)

[System Watcher](#)

[Acerca de System Watcher](#)

[Activación y desactivación de System Watcher](#)

[Configurar System Watcher](#)

[Activar o desactivar la protección contra exploits](#)

[Elija una acción en caso de que se detecte actividad maliciosa en un programa](#)

[Activación y desactivación de la anulación de acciones de malware durante la desinfección](#)

[Firewall](#)

[Acerca de Firewall](#)

[Activación y desactivación de Firewall](#)

[Acerca de las reglas de red](#)

[Acerca del estado de la conexión de red](#)

[Modificación del estado de la conexión de red](#)

[Gestión de las reglas de paquetes de red](#)

[Creación y edición de una regla de paquetes de red](#)

[Activación o desactivación de una regla de paquetes de red](#)

[Modificación de la acción de Firewall para una regla de paquetes de red](#)

[Modificación de la prioridad de una regla de paquetes de red](#)

[Gestionar reglas de red de la aplicación](#)

[Creación y edición de una regla de red para una aplicación](#)

[Activar y desactivar una regla de red de la aplicación](#)

[Modificación de la acción de Firewall para una regla de red de la aplicación](#)

[Modificación de la prioridad de una regla de red de la aplicación](#)

[Monitor de red](#)

[Acerca de Monitor de red](#)

[Inicio de Monitor de red](#)

[Prevención de intrusiones](#)

[Acerca de Prevención de intrusiones](#)

[Activación y desactivación de Prevención de intrusiones](#)

[Parámetros de prevención de intrusiones](#)

[Edición de la configuración utilizada para bloquear un equipo atacante](#)

[Configurar direcciones de exclusiones de bloqueo](#)

[Prevención de ataques de BadUSB](#)

[Acerca de Prevención de ataques de BadUSB](#)

[Instalación del componente Prevención de ataques de BadUSB](#)

[Activación y desactivación de Prevención de ataques de BadUSB](#)

[Permiso y prohibición de uso del teclado en pantalla para la autorización](#)

[Autorización del teclado](#)

[Control de inicio de aplicaciones](#)

[Acerca de Control de inicio de aplicaciones](#)

[Activación y desactivación de Control de inicio de aplicaciones](#)

[Limitaciones de funcionalidad de Control de inicio de aplicaciones](#)

[Acerca de las reglas de Control de inicio de aplicaciones](#)

[Gestión de reglas de Control de inicio de aplicaciones](#)

[Adición y edición de una regla de Control de inicio de aplicaciones](#)

[Adición de una condición de activación para una regla de Control de inicio de aplicaciones](#)

[Cambiar el estado de una regla de Control de inicio de aplicaciones](#)

[Probar reglas de Control de inicio de aplicaciones](#)

[Edición de plantillas de mensajes de Control de inicio de aplicaciones](#)

[Acerca de los modos de funcionamiento de Control de inicio de aplicaciones](#)

[Seleccionar el modo de Control de inicio de aplicaciones](#)

[Gestionar reglas de Control de inicio de aplicaciones con Kaspersky Security Center](#)

[Recopilación de información acerca de las aplicaciones instaladas en los equipos de los usuarios](#)

[Creación de categorías de aplicaciones](#)

[Crear reglas de Control de inicio de aplicaciones con Kaspersky Security Center](#)

[Cambio del estado de una regla de Control de inicio de aplicaciones mediante Kaspersky Security Center](#)

[Control de actividad de aplicaciones](#)

[Acerca de Control de actividad de aplicaciones](#)

[Limitaciones del control de dispositivos de audio y de vídeo](#)

[Activación y desactivación de Control de actividad de aplicaciones](#)

[Gestionar grupos de confianza de aplicaciones](#)

[Configurar los ajustes para asignar aplicaciones a grupos de confianza](#)

[Modificación de un grupo de confianza](#)

[Seleccionar un grupo de confianza para aplicaciones iniciadas antes que Kaspersky Endpoint Security.](#)

[Gestión de reglas de Control de aplicaciones](#)

[Cambiar reglas de control de aplicaciones para grupos de confianza y grupos de aplicaciones](#)

[Edición de una regla de control de aplicaciones](#)

[Desactivación de las descargas y actualizaciones de reglas de control de aplicaciones desde la base de datos de Kaspersky Security Network](#)

[Desactivación de la herencia de restricciones del proceso principal](#)

[Exclusión de acciones de aplicaciones concretas desde las reglas de control de aplicaciones](#)

[Eliminar reglas de control de aplicaciones obsoletas](#)

[Protección de recursos del sistema operativo y de datos de identidad](#)

[Adición de una categoría de recursos protegidos](#)

[Adición de un recurso protegido](#)

[Desactivación de la protección de un recurso](#)

[Control de vulnerabilidades](#)

[Acerca del Control de vulnerabilidades](#)

[Activación y desactivación del Control de vulnerabilidades](#)

[Control de dispositivos](#)

[Acerca del Control de dispositivos](#)

[Activación y desactivación del Control de dispositivos](#)

[Acerca de las reglas de acceso a dispositivos y a buses de conexión](#)

[Acerca de dispositivos de confianza](#)

[Decisiones estándar sobre el acceso a dispositivos](#)

[Edición de una regla de acceso a dispositivos](#)

[Agregar o excluir archivos al registro del evento o desde él](#)

[Agregar una red Wi-Fi a la lista de confianza](#)

[Edición de una regla de acceso a bus de conexión](#)

[Acciones con dispositivos de confianza](#)

[Adición de un dispositivo a la lista de confianza en la interfaz de la aplicación](#)

[Adición de dispositivos a la lista de confianza según el modelo o el ID del dispositivo](#)

[Adición de dispositivos a la lista de confianza según la máscara del ID de dispositivo](#)

[Configuración del acceso de usuario a un dispositivo de confianza](#)

[Eliminación de un dispositivo de la lista de dispositivos de confianza](#)

[Edición de plantillas de mensajes de Control de dispositivos](#)

[Obtención de acceso a un dispositivo bloqueado](#)

[Crear una clave para acceder a un dispositivo bloqueado mediante Kaspersky Security Center](#)

[Control Web](#)

[Acerca de Control Web](#)

[Activación y desactivación de Control Web](#)

[Categorías de contenido de recursos web](#)

[Acerca de las reglas de acceso a recursos web](#)

[Acciones con reglas de acceso a recursos web](#)

[Adición y edición de reglas de acceso a recursos web](#)

[Asignación de prioridades a reglas de acceso a recursos web](#)

[Comprobación de las reglas de acceso a recursos web](#)

[Activación y desactivación de una regla de acceso a recursos web](#)

[Migración de reglas de acceso a recursos web de las versiones previas de la aplicación](#)

[Exportación e importación de la lista de direcciones de recursos web](#)

[Edición de máscaras para direcciones de recursos web](#)

[Edición de plantillas de mensajes de Control Web](#)

[Sensor de endpoint de KATA](#)

[Acerca del sensor de endpoint de KATA](#)

[Activación y desactivación del componente Sensor de endpoint de KATA](#)

[Cifrado de datos](#)

[Activación de la visualización de la configuración del cifrado de la directiva de Kaspersky Security Center](#)

[Acerca del cifrado de datos](#)

[Limitaciones de funcionalidad del cifrado](#)

[Cambio del algoritmo de cifrado](#)

[Activación de la tecnología de inicio de sesión único \(SSO\)](#)

[Consideraciones especiales para el cifrado de archivos](#)

[Cifrado de los archivos de las unidades del equipo local](#)

[Cifrado de los archivos de las unidades del equipo local](#)

[Creación de reglas de acceso a archivos cifrados para aplicaciones](#)

[Cifrar archivos creados o modificados por aplicaciones específicas](#)

[Generación de una regla de descifrado](#)

[Descifrado de archivos de las unidades del equipo local](#)

[Creación de paquetes cifrados](#)

[Extracción de los paquetes cifrados](#)

[Cifrado de unidades extraíbles](#)

[Iniciar el cifrado de unidades extraíbles](#)

[Agregar una regla de cifrado para unidades extraíbles](#)

[Editar una regla de cifrado para unidades extraíbles](#)

[Activación del modo portátil para acceder a archivos cifrados de unidades extraíbles](#)

[Descifrado de unidades extraíbles](#)

[Cifrado de discos duros](#)

[Acerca del cifrado de discos duros](#)

[Cifrado de discos duros mediante la tecnología Cifrado de disco de Kaspersky](#)

[Cifrar discos duros mediante la tecnología Cifrado de unidad BitLocker](#)

[Creación de una lista de discos duros excluidos del cifrado](#)

[Descifrado de discos duros](#)

[Gestionar el Agente de autenticación](#)

[Utilizar una tarjeta inteligente y un token con el Agente de autenticación](#)

[Editar los mensajes de ayuda del Agente de autenticación](#)

[Compatibilidad limitada con los caracteres de los mensajes de ayuda del Agente de autenticación](#)

[Seleccionar el nivel de rastreo del Agente de autenticación](#)

[Administración de cuentas del Agente de autenticación](#)

[Adición de un comando para crear una cuenta del Agente de autenticación](#)

[Agregar un comando de modificación de cuentas del Agente de autenticación](#)

[Agregar un comando para eliminar una cuenta del Agente de autenticación](#)

[Restaurar las credenciales de la cuenta del Agente de autenticación](#)

[Responder a un usuario que solicita restaurar las credenciales de la cuenta del Agente de autenticación](#)

[Visualización de los detalles del cifrado de datos](#)

[Acerca del estado del cifrado](#)

[Ver el estado de cifrado](#)

[Ver el estado de cifrado en los paneles de información de Kaspersky Security Center](#)

[Ver errores de cifrado de archivos en unidades del equipo local](#)

[Visualización del informe del cifrado de datos](#)

[Administración de archivos con una funcionalidad de cifrado de archivos limitada](#)

[Acceso a archivos cifrados sin conexión a Kaspersky Security Center](#)

[Conceder acceso a archivos cifrados sin conexión a Kaspersky Security Center](#)

[Modificación de plantillas de mensajes de acceso a archivos cifrados](#)

[Trabajar con dispositivos cifrados cuando no hay acceso a estos](#)

[Obtención de acceso a dispositivos cifrados a través de la interfaz de aplicación](#)

[Conceder al usuario acceso a dispositivos cifrados](#)

[Proporcionar a un usuario una clave de recuperación para discos duros cifrados con BitLocker](#)

[Creación del archivo ejecutable de la Utilidad de restauración](#)

[Restaurar datos en dispositivos cifrados por medio de la Utilidad de restauración](#)

[Responder a un usuario que solicita restaurar datos de dispositivos cifrados](#)

[Restauración del acceso a los datos cifrados después del error del sistema operativo](#)

[Creación de un disco de rescate del sistema operativo](#)

[Protección de red](#)

[Acerca de Protección de red](#)

[Configuración de los parámetros de supervisión del tráfico de red](#)

[Activación de la vigilancia de todos los puertos de red](#)

[Creación de una lista de puertos de red supervisados](#)

[Creación de una lista de aplicaciones para las que se supervisan todos los puertos de red](#)

[Actualización de las bases de datos y módulos de la aplicación](#)

[Acerca de las actualizaciones de la base de datos y de los módulos de la aplicación](#)

[Acerca de los orígenes de actualizaciones](#)

[Configuración de los parámetros de actualización](#)

[Adición de un origen de actualizaciones](#)

[Selección de la región del servidor de actualización](#)

[Configuración de actualización desde una carpeta compartida](#)

[Selección del modo de ejecución de la tarea de actualización](#)

[Inicio de una tarea de actualización con los permisos de una cuenta de usuario distinta](#)

[Configurar las actualizaciones de los módulos de la aplicación](#)

[Inicio y parada de una tarea de actualización](#)

[Anulación de la última actualización](#)

[Configuración de los parámetros del servidor proxy](#)

[Análisis del equipo](#)

[Acerca de las tareas de análisis](#)

[Inicio o detención de una tarea de análisis](#)

[Configuración de los parámetros de las tareas de análisis](#)

[Cambiar el nivel de seguridad](#)

[Modificación de las acciones que se van a realizar en archivos infectados](#)

[Generación de una lista de objetos para analizar](#)

[Selección del tipo de archivo que se va a analizar](#)

[Optimización del análisis de archivos](#)

[Análisis de archivos compuestos](#)

[Uso de métodos de análisis](#)

[Uso de tecnologías de análisis](#)

[Seleccionar el modo de ejecución para la tarea de análisis](#)

[Inicio de una tarea de análisis con la cuenta de un usuario distinto](#)

[Análisis de unidades extraíbles cuando se conectan al equipo](#)

[Gestión de archivos sin procesar](#)

[Acerca de los archivos sin procesar](#)

[Gestión de la lista de archivos sin procesar](#)

[Inicio de una tarea de análisis personalizado para archivos sin procesar](#)

[Eliminación de archivos de la lista de archivos sin procesar](#)

[Análisis de vulnerabilidades](#)

[Visualización de información sobre vulnerabilidades de aplicaciones en ejecución](#)

[Acerca de la tarea Análisis de vulnerabilidades](#)

[Inicio o detención de la tarea Análisis de vulnerabilidades](#)

[Configurar los ajustes de Análisis de vulnerabilidades](#)

[Creación de la cobertura del análisis de vulnerabilidades](#)

[Seleccionar el modo de ejecución para la tarea de Análisis de vulnerabilidades](#)

[Iniciar una tarea de análisis de vulnerabilidades con los permisos de una cuenta de usuario distinta](#)

[Gestión de la lista de vulnerabilidades](#)

[Acerca de la lista de vulnerabilidades](#)

[Nuevo inicio de la tarea Análisis de vulnerabilidades](#)

[Arreglo de vulnerabilidades](#)

[Ocultación de entradas en la lista de vulnerabilidades](#)

[Filtrado de la lista de vulnerabilidades por nivel de gravedad](#)

[Filtrado de la lista de vulnerabilidades por valores de estado Arreglado u Oculto](#)

[Comprobar la integridad de los módulos de la aplicación](#)

[Acerca de la tarea Comprobación de integridad](#)

[Iniciar o detener una tarea de comprobación de integridad](#)

[Seleccionar el modo de ejecución para la tarea de comprobación de la integridad](#)

[Gestión de informes](#)

[Principios de la gestión de informes](#)

[Configuración de los parámetros de los informes](#)

[Configuración del período máximo de almacenamiento del informe](#)

[Configuración del tamaño máximo del archivo del informe](#)

[Visualización de informes](#)

[Ver información de eventos en un informe](#)

[Almacenamiento de informes en archivos](#)

[Limpieza de informes](#)

[Servicio de notificaciones](#)

[Acerca de las notificaciones de Kaspersky Endpoint Security.](#)

[Configuración del servicio de notificaciones](#)

[Configuración de los parámetros de registro de eventos](#)

[Configuración de la visualización y entrega de notificaciones](#)

[Configuración de la visualización de advertencias sobre el estado de la aplicación en el área de notificaciones](#)

[Gestión de Cuarentena y Respaldo](#)

[Acerca de Cuarentena y Respaldo](#)

[Configuración de los parámetros de Cuarentena y Respaldo](#)

[Configuración del período de almacenamiento máximo de archivos en Cuarentena y de las copias de archivos en Respaldo](#)

[Configuración del tamaño máximo de Cuarentena y Respaldo](#)

[Gestión de Cuarentena](#)

[Activación y desactivación del análisis de archivos en Cuarentena tras una actualización](#)

[Inicio de una tarea de análisis personalizado para archivos en Cuarentena](#)

[Restauración de archivos de la Cuarentena](#)

[Eliminación de archivos de la Cuarentena](#)

[Gestión de Respaldo](#)

[Restauración de archivos de Respaldo](#)

[Eliminación de las copias de seguridad de los archivos de Respaldo](#)

[Configuración avanzada de la aplicación](#)

[Crear y utilizar un archivo de configuración](#)

[Zona de confianza](#)

[Acerca de la zona de confianza](#)

[Creación de una exclusión del análisis](#)

[Modificación de una exclusión del análisis](#)

[Eliminación de una exclusión del análisis](#)

[Activación y desactivación de una exclusión del análisis](#)

[Edición de la lista de aplicaciones de confianza](#)

[Activación y desactivación de reglas de la zona de confianza para una aplicación en la lista de aplicaciones de confianza](#)

[Uso del almacén de certificados de confianza del sistema](#)

[Autoprotección de Kaspersky Endpoint Security](#)

[Acerca de la Autoprotección de Kaspersky Endpoint Security.](#)

[Activación y desactivación de la Autoprotección](#)

[Activación o desactivación de Protección de control remoto](#)

[Soporte de las aplicaciones de administración remota](#)

[Rendimiento de Kaspersky Endpoint Security y compatibilidad con otras aplicaciones](#)

[Acerca de rendimiento de Kaspersky Endpoint Security y compatibilidad con otras aplicaciones](#)

[Selección de los tipos de objetos detectables](#)

[Activación o desactivación de la tecnología de desinfección avanzada de estaciones de trabajo](#)

[Activación o desactivación de la tecnología de desinfección avanzada de servidores de archivos](#)

[Activación o desactivación del modo de ahorro de energía](#)

[Activación o desactivación de la concesión de recursos a otras aplicaciones](#)

[Protección con contraseña](#)

[Acerca del acceso restringido a Kaspersky Endpoint Security.](#)

[Activación y desactivación de la protección con contraseña](#)

[Modificación de la contraseña de acceso a Kaspersky Endpoint Security.](#)

[Acerca de la utilización de una contraseña temporal](#)

[Crear una contraseña temporal utilizando la consola de administración de Kaspersky Security Center](#)

[Aplicar una contraseña temporal en la interfaz de Kaspersky Endpoint Security.](#)

[Administración remota de la aplicación con Kaspersky Security Center](#)

[Acerca de la administración de la aplicación a través de Kaspersky Security Center](#)

[Consideraciones especiales al trabajar con versiones diferentes de complementos de administración](#)

[Ejecución y detención de Kaspersky Endpoint Security en un equipo cliente](#)

[Configuración de los parámetros de Kaspersky Endpoint Security.](#)

[Gestión de tareas](#)

[Acerca de las tareas para Kaspersky Endpoint Security.](#)

[Configuración del modo de administración de tareas](#)

[Creación de una tarea local](#)

[Creación de una tarea de grupos](#)

[Crear una tarea para selección de dispositivos](#)

[Ejecución, interrupción, suspensión y reanudación de una tarea](#)

[Edición de la configuración de tareas](#)

[Gestión de directivas](#)

[Acerca de las directivas](#)

[Creación de una directiva](#)

[Edición de la configuración de directivas](#)

[Selección de los ajustes que se mostrarán en la política de Kaspersky Security Center](#)

[Enviar mensajes del usuario al servidor de Kaspersky Security Center](#)

[Visualización de los mensajes del usuario en el almacén de eventos de Kaspersky Security Center](#)

[Participación en Kaspersky Security Network](#)

[Acerca de la participación en Kaspersky Security Network](#)

[Activación y desactivación del uso de Kaspersky Security Network](#)

[Comprobación de la conexión a Kaspersky Security Network](#)

[Comprobar la reputación de un archivo en Kaspersky Security Network](#)

[Protección mejorada con Kaspersky Security Network](#)

[Fuentes de información de la aplicación](#)

[Cómo ponerse en contacto con el Soporte técnico](#)

[Cómo obtener soporte técnico](#)

[Soporte técnico por teléfono](#)

[Soporte técnico a través de CompanyAccount de Kaspersky.](#)

[Recopilación de información para el Soporte técnico](#)

[Creación de un archivo de depuración](#)

[Contenido y almacenamiento de archivos de seguimiento](#)

[Activar o desactivar el envío de archivos de volcado y rastreo a Kaspersky.](#)

[Enviar archivos al servidor de Soporte técnico](#)

[Glosario](#)

[Actualización](#)

[Administrador de archivos portátiles](#)

[Agente de autenticación](#)

[Agente de red](#)

[Análisis de firmas](#)

[Análisis heurístico](#)

[Archivador](#)

[Archivo infectable](#)

[Archivo infectado](#)

[Archivo probablemente infectado](#)

[Base de datos de direcciones web fraudulentas](#)

[Base de datos de direcciones web maliciosas](#)

[Bases de datos antivirus](#)

[Certificado](#)

[Certificado de la licencia](#)

[Clave activa](#)

[Clave adicional](#)

[Cobertura de protección](#)

[Cobertura del análisis](#)

[Conector del agente de red](#)

[Configuración de la aplicación](#)

[Configuración de tareas](#)

[Cuarentena](#)

[Desinfección](#)

[Emisor del certificado](#)

[Exploits](#)

[Falsa alarma](#)

[Forma normalizada de la dirección de un recurso web](#)

[Grupo de administración](#)

[Huella digital del certificado](#)

[Lista negra de direcciones](#)

[Máscara de archivos](#)

[Módulo de plataforma segura](#)

[Módulos de la aplicación](#)

[Movimiento de archivos a Cuarentena](#)

[Objeto OLE](#)

[Parche](#)

[Phishing](#)

[Respaldo](#)

[Servicio de red](#)

[Servidor de administración](#)

[Sujeto del certificado](#)

[Tarea](#)

[Información sobre el código de terceros](#)

[Información de marcas registradas](#)

Acerca de Kaspersky Endpoint Security 10 Service Pack 2 para Windows

Esta sección describe las funciones, componentes y el kit de distribución de Kaspersky Endpoint Security e incluye una lista de requisitos de hardware y software de Kaspersky Endpoint Security.

Novedades

Kaspersky Endpoint Security 10 Service Pack 2 para Windows ofrece las siguientes funciones y mejoras:

1. Control de inicio de aplicaciones:

- Admite sistemas operativos de servidores.
- Controla las descargas de módulos DLL y controladores.
- Administra la lista de objetos en la tarea de inventario (módulos DLL y archivos del script).
- Controla objetos basados en un nuevo criterio: según los atributos de los certificados de firma digital.
- Genera un informe sobre inicios de prueba de aplicaciones bloqueadas.
- Admite dos modos de funcionamiento para Control de inicio de aplicaciones: "Lista negra" y "Lista blanca".
- Usa el hash SHA256 para control e inventario de objetos.
- Controla la ejecución de scripts desde el intérprete de PowerShell.
- Utiliza el almacenamiento certificado de confianza del sistema.

2. La administración de Microsoft BitLocker activa discos duros de cifrado con la ayuda de la tecnología de BitLocker de Microsoft:

- Administre el cifrado de forma remota.
- Supervise dispositivos cifrados.
- Cree informes de cifrado de dispositivos.
- Restaure el acceso a los dispositivos cifrados.

3. Cifrado de disco de Kaspersky:

- Compatibilidad con la entrada de credenciales en el entorno anterior al arranque del Agente de autenticación mediante un teclado virtual.
- Compatibilidad con el modo de cifrado para cifrar sólo el espacio ocupado en un dispositivo.
- Compatibilidad con el cifrado en tabletas (MS Surface versiones 3 y 4).

4. Control de actividad de aplicaciones:

- Controla el acceso de aplicaciones a dispositivos de grabación de audio y vídeo.

5. Control Web:

- Configura reglas de acceso a recursos web para categorías adicionales de recursos web.

6. Control de dispositivos:

- Registra eventos asociados con la eliminación y el almacenamiento de archivos en dispositivos USB.
- Genera una lista de redes Wi-Fi de confianza según la configuración siguiente: nombre, tipo de cifrado y tipo de autenticación.
- Administra los derechos del acceso del usuario para las operaciones de lectura y escritura de archivos en CD y DVD.

7. Antivirus del correo:

- Capaz de eliminar y renombrar tipos concretos de archivos dentro de comprimidos para analizar con Antivirus del correo.

8. Kaspersky Security Network:

- Muestra KSN como una razón para tomar una decisión en relación con el método de procesamiento de objetos en informes de Kaspersky Endpoint Security e informes de Kaspersky Security Center.
- Envía una consulta a KSN sobre la reputación de un archivo seleccionado.
- Muestra un estado de disponibilidad de servidores de KSN para equipos del cliente que tengan instalado Kaspersky Endpoint Security.

Kit de distribución

El kit de distribución de Kaspersky Endpoint Security contiene los siguientes archivos:

- Archivos necesarios para [instalar la aplicación](#) mediante alguno de los siguientes métodos:
- Archivos del paquete de actualización utilizados durante la instalación de la aplicación.
- El archivo klcfginst.msi para instalar el complemento de administración Kaspersky Endpoint Security mediante Kaspersky Security Center.
- El archivo ksn_<ID de idioma>.txt, en el que puede consultar los términos de [participación en Kaspersky Security Network](#).
- El archivo license.txt, con el cual puede ver el [contrato de licencia de usuario final](#).
- El archivo incompatible.txt que contiene una lista con el software que no es compatible.
- El archivo installer.ini, que contiene la configuración interna del kit de distribución.

No se recomienda cambiar los valores de esta configuración. Si desea cambiar las opciones de instalación, utilice el archivo [setup.ini](#).

Debe desempaquetar el kit de distribución para acceder a los archivos.

Organización de la protección del equipo

Kaspersky Endpoint Security ofrece una protección completa al equipo frente a varios tipos de amenazas, ataques de red e intentos de suplantación de identidad (phishing).

Un componente específico gestiona cada tipo de amenaza. Los componentes se pueden activar o desactivar de forma independiente y es posible configurar su configuración.

Además de la protección en tiempo real que ofrecen los componentes de la aplicación, es recomendable que *analice* regularmente el equipo en busca de virus y otras amenazas. Esto ayuda a descartar la posibilidad de que se extienda el software malicioso (malware) que los componentes de protección no han detectado debido a una configuración de nivel de seguridad baja o a otros motivos.

Para mantener actualizado Kaspersky Endpoint Security, debe *actualizar* las bases de datos y los módulos que la aplicación utiliza. De forma predeterminada, la aplicación se actualiza automáticamente, pero, si es necesario, puede actualizar las bases de datos y los módulos de la aplicación manualmente.

Los siguientes componentes de aplicaciones son componentes de control:

- **Control de inicio de aplicaciones.** Este componente realiza un seguimiento de los intentos del usuario de iniciar aplicaciones y regula el inicio de aplicaciones.
- **Control de actividad de aplicaciones.** Este componente registra las acciones de las aplicaciones del sistema operativo y regula la actividad de las aplicaciones en función del grupo de confianza de una aplicación determinada. Se especifica un conjunto de reglas para cada grupo de aplicaciones. Estas reglas regulan el acceso de las aplicaciones a los datos del usuario y a los recursos del sistema operativo. Entre estos datos se incluyen los archivos de usuario (carpeta Mis documentos, cookies, información sobre las actividades del usuario) y archivos, carpetas y claves de registro que contienen configuración e información importante sobre las aplicaciones que más se utilizan.
- **Control de vulnerabilidades.** El componente Control de vulnerabilidades ejecuta un análisis de vulnerabilidades en tiempo real de aplicaciones que se han iniciado o que se están ejecutando en el equipo del usuario.
- **Control de dispositivos.** Este componente permite definir restricciones flexibles en el acceso a dispositivos de almacenamiento de datos (como unidades de disco duro, unidades extraíbles, unidades de cinta, y discos CD y DVD), equipos de transmisión de datos (como módems), equipos que convierten información en copias impresas (como impresoras) o interfaces para conectar dispositivos a equipos (como USB, Bluetooth e infrarrojos).
- **Control Web.** Este componente permite definir restricciones flexibles en el acceso a recursos web para diferentes grupos de usuarios.

El funcionamiento de los componentes de control se basa en las siguientes reglas:

- El Control de inicio de aplicaciones utiliza [Reglas de Control de inicio de aplicaciones](#).
- El Control de actividad de aplicaciones utiliza [Reglas de Control de aplicaciones](#).
- El Control de dispositivos utiliza [reglas de acceso a dispositivos y reglas de acceso a buses de conexión](#).
- El Control Web utiliza [reglas de acceso a recursos web](#).

Los siguientes componentes de aplicaciones son componentes de protección:

- **Antivirus de archivos.** Este componente protege el equipo frente a la infección del sistema de archivos. Antivirus de archivos se inicia junto con Kaspersky Endpoint Security, permanece activo todo el tiempo en la memoria del equipo y analiza todos los archivos que se abran, se guarden o se ejecuten en el equipo y en todas las unidades conectadas. Antivirus de archivos intercepta cada intento de acceso a un archivo y analiza el archivo en busca de virus y otras amenazas.
- **System Watcher.** Este componente mantiene un registro de la actividad de la aplicación en el equipo y proporciona información a otros componentes para garantizar una protección más efectiva del equipo.
- **Antivirus del correo.** Este componente analiza mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenazas.
- **Antivirus Internet.** Este componente analiza el tráfico que llega al equipo del usuario mediante los protocolos HTTP y FTP, y comprueba si las URL están incluidas en listas de direcciones web maliciosas o fraudulentas.
- **Antivirus para chat.** Este componente analiza el tráfico que llega al equipo mediante protocolos de clientes de mensajería instantánea. El componente le permite utilizar numerosos clientes de mensajería instantánea de forma segura.
- **Firewall.** Este componente protege los datos que se almacenan en el equipo y bloquea la mayoría de las posibles amenazas al sistema operativo mientras el equipo está conectado a Internet o a una red de área local. El componente filtra toda la actividad de red según estos dos tipos de reglas: [reglas de red para aplicaciones y reglas de paquetes de red](#).
- **Monitor de red.** Este componente permite ver la actividad de red del equipo en tiempo real.
- **Prevención de intrusiones.** Este componente inspecciona el tráfico de red entrante en busca de actividad que sea típica de ataques de red. Al detectar un intento de ataque de red dirigido a su equipo, Kaspersky Endpoint Security bloquea la actividad de red del equipo atacante.

Las siguientes tareas se proporcionan en Kaspersky Endpoint Security:

- **Análisis completo.** Kaspersky Endpoint Security analiza el sistema operativo, incluidos la RAM, objetos que se cargan al iniciarse, el almacenamiento de copias de seguridad del sistema operativo y todas las unidades de disco duro y extraíbles.
- **Análisis personalizado.** Kaspersky Endpoint Security analiza los objetos seleccionados por el usuario.
- **Análisis de áreas críticas.** Kaspersky Endpoint Security analiza los objetos que se cargan al iniciarse el sistema operativo, la RAM y los objetos a los que van dirigidos procesos ocultos.
- **Actualización.** Kaspersky Endpoint Security descarga bases de datos y módulos de la aplicación actualizados. La actualización mantiene el equipo protegido contra los virus más recientes y otras amenazas.
- **Análisis de vulnerabilidades.** Kaspersky Endpoint Security analiza el sistema operativo y el software instalado en busca de vulnerabilidades. Este análisis garantiza una detección y eliminación puntual de posibles problemas que los intrusos pueden utilizar.

La funcionalidad de cifrado de archivos le permite cifrar los archivos y las carpetas que se almacenan en las unidades del equipo local. La funcionalidad de cifrado de unidades le permite cifrar los discos duros y las unidades extraíbles.

Administración remota a través de Kaspersky Security Center

Kaspersky Security Center permite iniciar y detener de forma remota Kaspersky Endpoint Security en el equipo de un cliente, así como gestionar y configurar los parámetros de la aplicación de forma remota.

Funciones de servicio de la aplicación

Kaspersky Endpoint Security incluye varias funciones de servicio. La finalidad de las funciones de servicio es mantener actualizada la aplicación, ampliar la funcionalidad y ayudar al usuario a utilizarla.

- **Informes.** Cuando se utiliza, la aplicación guarda un informe sobre cada componente de la aplicación y tarea. El informe contiene una lista de eventos de Kaspersky Endpoint Security y todas las operaciones que la aplicación realiza. Si se produce un incidente, puede enviar informes a Kaspersky, donde los especialistas del Soporte técnico pueden analizar el problema con más detenimiento.
- **Almacenamiento de datos.** Si la aplicación detecta archivos infectados o que probablemente lo estén mientras se analiza el equipo en busca de virus y otras amenazas, los bloqueará. Kaspersky Endpoint Security mueve los probablemente infectados a un almacenamiento especial denominado *Cuarentena*. Kaspersky Endpoint Security almacena copias de los archivos desinfectados y eliminados en *Copia de seguridad*. Kaspersky Endpoint Security mueve los archivos que no se procesan por algún motivo a la *lista de archivos sin procesar*. Puede analizar archivos, restaurarlos en sus carpetas originales y vaciar el almacenamiento de datos.
- **Servicio de notificaciones.** El servicio de notificaciones mantiene al usuario informado sobre el estado de la protección actual del equipo y el funcionamiento de Kaspersky Endpoint Security. Las notificaciones se pueden mostrar en la pantalla o se pueden enviar por correo electrónico.
- **Kaspersky Security Network.** La participación del usuario en Kaspersky Security Network mejora la efectividad de la protección del equipo a través de la recopilación en tiempo real de información sobre la reputación de archivos, recursos web y software de usuarios de todo el mundo.
- **Licencia.** La compra de una licencia desbloquea la funcionalidad completa de la aplicación, proporciona acceso a las actualizaciones de la base de datos y de los módulos de la aplicación, y ofrece soporte por teléfono o a través de correo electrónico para problemas relacionados con la instalación, la configuración y el uso de la aplicación.
- **Soporte.** Todos los usuarios registrados de Kaspersky Endpoint Security pueden ponerse en contacto con los especialistas del Soporte técnico para obtener ayuda. Puede enviar una solicitud desde su Cuenta Kaspersky del sitio web del Soporte técnico o recibir ayuda del personal de soporte técnico por teléfono.

Si la aplicación devuelve un error o se cuelga durante el funcionamiento, puede reiniciarse automáticamente.

Si la aplicación encuentra errores recurrentes que provocan el fallo de la aplicación, esta realiza las operaciones siguientes:

1. Desactiva las funciones de control y protección (la funcionalidad de cifrado permanece activa).
2. Informa al usuario de que las funciones se han desactivado.
3. Trata de restablecer la funcionalidad de la aplicación después de actualizar las bases de datos de antivirus o de aplicar las actualizaciones de los módulos de la aplicación.

La aplicación recibe información sobre errores periódicos y el sistema se cuelga mediante algoritmos definidos expresamente por los expertos de Kaspersky.

Requisitos de hardware y software

Para garantizar el funcionamiento adecuado de Kaspersky Endpoint Security, el equipo debe cumplir los siguientes requisitos:

Requisitos generales mínimos:

- 2 GB de espacio libre en disco en la unidad de disco duro
- Procesador con una velocidad de reloj de 1 GHz (compatible con el conjunto de instrucciones SSE2)
- RAM:
 - 1 GB para sistemas operativos de 32 bits;
 - 2 GB para sistemas operativos de 64 bits

Sistemas operativos admitidos para equipos personales:

- Windows 7 Home/Professional/Ultimate/Enterprise Service Pack 1 o versiones posteriores;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Education / Enterprise.

Para más información sobre la compatibilidad con el sistema operativo Microsoft Windows 10, visite la [Base de conocimientos del Servicio de soporte técnico](#).

Sistemas operativos admitidos para servidores de archivos:

- Windows Small Business Server 2008 Standard o Premium (64 bits);
- Windows Small Business Server 2011 Essentials o Standard (64 bits);
- Windows MultiPoint Server 2011 (64 bits);
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 o versiones posteriores;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 o versiones posteriores;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

Para más información sobre la compatibilidad con Microsoft Windows Server 2016 y Microsoft Windows Server 2019, visite la [Base de conocimientos del Servicio de soporte técnico](#).

Instalación y eliminación de la aplicación

Esta sección le guía a través de la instalación de Kaspersky Endpoint Security en el equipo, la realización de la configuración inicial, la actualización desde una versión anterior de la aplicación y la eliminación de la aplicación del equipo.

Instalación de la aplicación

Esta sección describe cómo instalar Kaspersky Endpoint Security en el equipo y cómo completar la configuración inicial de la aplicación.

Acerca de las formas de instalar la aplicación

Kaspersky Endpoint Security 10 para Windows se puede instalar de forma local (directamente en el equipo del usuario) o de forma remota desde la estación de trabajo del administrador.

Se puede realizar la instalación local de Kaspersky Endpoint Security 10 para Windows mediante uno de los modos siguientes:

- En modo interactivo, mediante el Asistente de instalación de la aplicación.
El modo interactivo requiere implicación por su parte en el proceso de instalación.
- En modo silencioso [desde la línea de comandos](#).
Una vez que la instalación se inicie en el modo silencioso, su participación en el proceso de instalación ya no se requiere.

La aplicación se puede instalar remotamente en ordenadores en red utilizando lo siguiente:

- Paquete de software Kaspersky Security Center (consulte la *Guía de implementación de Kaspersky Security Center*).
- El Editor de directivas de grupo de Microsoft Windows (consulte los archivos de ayuda del sistema operativo).
- [System Center Configuration Manager](#).

Le recomendamos que cierre todas las aplicaciones activas antes de comenzar la instalación de Kaspersky Endpoint Security (incluida la instalación remota).

Instalación de la aplicación mediante el Asistente de instalación

La interfaz del Asistente de configuración de aplicaciones consta de una secuencia de ventanas correspondientes a los pasos de instalación de la aplicación. Puede navegar por las páginas del Asistente de instalación utilizando los botones **Atrás** y **Siguiente**. Para cerrar el Asistente de instalación una vez que se complete la tarea, haga clic en el botón **Terminar**. Para interrumpir el Asistente de instalación en cualquier momento, haga clic en el botón **Cancelar**.

Para instalar la aplicación o actualizarla a partir de una versión anterior mediante el Asistente de instalación:

1. Ejecute el archivo setup.exe incluido en el [kit de distribución](#).

Se iniciará el Asistente de instalación.

2. Siga las instrucciones del Asistente de instalación.

Cuando se ejecuta el archivo setup.exe, Kaspersky Endpoint Security analiza el equipo en busca de cualquier software no compatible. De forma predeterminada, después de detectar software no compatible, el proceso de instalación se cancela y la lista de aplicaciones no compatibles con Kaspersky Endpoint Security aparece en la pantalla. Para continuar la instalación, elimine estas aplicaciones del equipo.

Paso 1. Asegúrese de que el equipo cumple con los requisitos de instalación

Antes de instalar Kaspersky Endpoint Security 10 para Windows en un equipo o actualizar una versión anterior de la aplicación, se comprueban las siguientes condiciones:

- Si el sistema operativo y el service pack cumplen con los [requisitos de software para la instalación del producto](#).
- Si se cumplen o no los [requisitos de hardware y software](#).
- Si el usuario tiene los derechos necesarios para instalar el producto de software.

Si alguno de los requisitos previos no se cumple, se muestra una notificación pertinente en pantalla.

Si el equipo cumple con los requerimientos arriba indicados, el Asistente de instalación buscará aplicaciones de Kaspersky que puedan provocar conflictos si se ejecutan al mismo tiempo que la aplicación que se va a instalar. Si se encuentran estas aplicaciones, se le pregunta si desea eliminarlas manualmente.

Si las aplicaciones detectadas incluyen versiones anteriores de Kaspersky Endpoint Security, todos los datos que se pueden migrar (por ejemplo, datos de activación y configuración de la aplicación) se conservan y se usan durante la instalación de Kaspersky Endpoint Security 10 Service Pack 2 para Windows, y la versión anterior de la aplicación se elimina automáticamente. Esto se aplica a las siguientes versiones de la aplicación:

- Kaspersky Anti-Virus 6.0 para Windows Workstations MP4 CF1 / MP4 CF2
- Kaspersky Anti-Virus 6.0 para Windows Servers MP4 / MP4 CF2
- Kaspersky Endpoint Security 10 Service Pack 1 para Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 para Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 para Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 para Windows

Paso 2. Página de bienvenida del proceso de instalación

Si se cumplen todos los requisitos para la instalación de la aplicación, aparecerá una página de bienvenida tras el inicio del paquete de instalación. La página de bienvenida indica el inicio de la instalación de Kaspersky Endpoint Security en el equipo.

Para seguir con el Asistente de instalación, haga clic en el botón **Siguiente**.

Paso 3. Visualización del Contrato de licencia

En este punto, le recomendamos que consulte el Contrato de licencia entre usted y Kaspersky.

Lea detenidamente el Contrato de licencia y, si está de acuerdo con todos los términos, seleccione la casilla de verificación **Acepto los términos del contrato de licencia**.

Para volver al paso anterior del Asistente de instalación, haga clic en el botón **Atrás**. Para seguir con el Asistente de instalación, haga clic en el botón **Siguiente**. Para interrumpir el Asistente de instalación, haga clic en el botón **Cancelar**.

Paso 4. Selección del tipo de instalación

En este momento, puede seleccionar el tipo de instalación de Kaspersky Endpoint Security Data Protection Suite que le resulte más conveniente:

- **Instalación básica.** Si elige este tipo de instalación, los componentes de protección, Control de actividad de aplicaciones y Control de vulnerabilidades se instalan en el equipo con la configuración recomendada por expertos de Kaspersky.
- **Instalación estándar.** Si elige este tipo de instalación, los componentes de la protección y del control con la configuración recomendada por Kaspersky se instalan en el equipo.
- **Instalación personalizada.** Si selecciona este tipo de instalación, se le solicita que seleccione los [componentes para instalar](#) y que especifique la [carpeta de destino de la aplicación](#).

Este tipo de instalación le permite instalar los componentes que no se incluyen en las instalaciones básicas y estándares.

La instalación estándar está seleccionada de forma predeterminada.

Para volver al paso anterior del Asistente de instalación, haga clic en el botón **Atrás**. Para seguir con el Asistente de instalación, haga clic en el botón **Siguiente**. Para interrumpir el Asistente de instalación, haga clic en el botón **Cancelar**.

Paso 5. Selección de los componentes de la aplicación que se van a instalar

Este paso se lleva a cabo si selecciona *Instalación personalizada* de la aplicación.

En este momento, puede seleccionar los componentes de Kaspersky Endpoint Security que desea instalar. Antivirus de archivos es un componente obligatorio para la instalación. No puede cancelar su instalación.

De forma predeterminada, se seleccionan todos los componentes de la aplicación para la instalación, a excepción de los siguientes:

- [Prevención de ataques de BadUSB](#).
- [Cifrado de disco](#).
- [Cifrado de archivos](#).

- [Administrador de Microsoft BitLocker](#).
- [Sensor de endpoint de KATA](#).

Administrador de Microsoft BitLocker realiza las funciones siguientes:

- Administra el cifrado de BitLocker integrado en el sistema operativo Windows.
- Configura los ajustes de la directiva de cifrado y comprueba su aplicabilidad para el equipo administrado.
- Inicia los procesos de cifrado y descifrado.
- Supervisa el estado del cifrado en el equipo administrado.
- Almacena de forma centralizada las claves de recuperación en el servidor de administración de Kaspersky Security Center.

El *sensor de endpoint de KATA* es un componente de la plataforma Kaspersky Anti Targeted Attack. Esta solución está destinada a la detección rápida de amenazas como ataques dirigidos. El componente supervisa continuamente los procesos, las conexiones de red activas y los archivos modificados, y envía esta información a la plataforma Kaspersky Anti Targeted Attack.

Para seleccionar la instalación de un componente, haga clic en el icono que se encuentra junto al nombre del componente para abrir el menú contextual y seleccionar **Esta función se instalará en el disco duro local**. Para obtener más detalles sobre las tareas que realiza el componente seleccionado y el espacio en disco duro que se requiere para instalar el componente, diríjase a la parte inferior de la página actual del Asistente de instalación.

Para ver información detallada sobre el espacio disponible en los discos duros locales, haga clic en el botón **Volumen**. La información se mostrará en la ventana **Espacio disponible en el disco** que aparece.

Para cancelar la instalación del componente, seleccione la opción **Esta función no estará disponible** del menú contextual.

Para volver a la lista de componentes instalados de forma predeterminada, haga clic en el botón **Restablecer**.

Para volver al paso anterior del Asistente de instalación, haga clic en el botón **Atrás**. Para seguir con el Asistente de instalación, haga clic en el botón **Siguiente**. Para interrumpir el Asistente de instalación, haga clic en el botón **Cancelar**.

Paso 6. Selección de la carpeta de destino

Este paso está disponible si selecciona la *Instalación personalizada* de la aplicación.

Durante este paso, puede especificar la ruta hacia la carpeta de destino donde se instalará la aplicación. Para seleccionar la carpeta de destino para la aplicación, haga clic en el botón **Examinar**.

Para ver información sobre el espacio disponible en los discos duros locales, haga clic en el botón **Volumen**. La información se muestra en la ventana **Requisitos de espacio en el disco** que aparece.

Para volver al paso anterior del Asistente de instalación, haga clic en el botón **Atrás**. Para seguir con el Asistente de instalación, haga clic en el botón **Siguiente**. Para interrumpir el Asistente de instalación, haga clic en el botón **Cancelar**.

Paso 7. Adición de exclusiones de análisis de virus

Este paso está disponible si selecciona la *Instalación personalizada* de la aplicación.

En este momento, puede especificar las exclusiones del análisis de virus que desea agregar a la configuración de la aplicación.

Las casilla de verificación **Excluir áreas recomendadas por Microsoft de la cobertura de análisis antivirus** / **Excluir áreas recomendadas por Kaspersky de la cobertura de análisis antivirus** excluyen, respectivamente, las áreas recomendadas por Microsoft o por Kaspersky de la zona de confianza o las incluyen.

Si se selecciona una de estas dos casillas de verificación, Kaspersky Endpoint Security incluye, respectivamente, las áreas que Microsoft o Kaspersky recomiendan en la zona de confianza. Kaspersky Endpoint Security no analiza esas áreas en busca de virus u otras amenazas.

La casilla de verificación **Excluir áreas recomendadas por Microsoft de la cobertura del análisis antivirus** está disponible cuando se instala Kaspersky Endpoint Security en un equipo que se ejecuta con Microsoft Windows para servidores de archivos.

Para volver al paso anterior del Asistente de instalación, haga clic en el botón **Atrás**. Para seguir con el Asistente de instalación, haga clic en el botón **Siguiente**. Para interrumpir el Asistente de instalación, haga clic en el botón **Cancelar**.

Paso 8. Preparación de la instalación de la aplicación

Se recomienda proteger el proceso de instalación porque su equipo puede infectarse con programas maliciosos que podrían interferir con la instalación de Kaspersky Endpoint Security 10 para Windows.

La protección del proceso de instalación está habilitada de forma predeterminada.

Sin embargo, si no se puede instalar la aplicación (por ejemplo, cuando se realiza la instalación remota con la ayuda del Escritorio remoto de Windows), se aconseja que desactive la protección del proceso de instalación. Si este es el caso, interrumpa la instalación y vuelva a iniciar el Asistente de instalación de la aplicación. En el paso "Preparación de la instalación de la aplicación", desactive la casilla de verificación **Proteger el proceso de instalación**.

La casilla de verificación **Garantizar compatibilidad con Citrix Provisioning Services** activa o desactiva la función que instala controladores en el modo de compatibilidad con Citrix PVS.

Seleccione esta casilla de verificación solo si trabaja con Citrix Provisioning Services.

La casilla de verificación **Agregue la ruta del archivo avp.com a la variable de entorno %PATH%** activa o desactiva una opción que agrega la ruta del archivo avp.com a la variable del sistema %PATH%.

Si se selecciona la casilla de verificación, el inicio de Kaspersky Endpoint Security o de cualquiera de sus tareas de la línea de comandos no requiere que se introduzca la ruta del archivo ejecutable. Basta con escribir el nombre del archivo ejecutable y el comando para iniciar una tarea en concreto.

Para volver al paso anterior del Asistente de instalación, haga clic en el botón **Atrás**. Para instalar el programa, haga clic en el botón **Instalar**. Para interrumpir el Asistente de instalación, haga clic en el botón **Cancelar**.

Las conexiones de red actuales podrían finalizar si la aplicación se está instalando en el equipo. La mayor parte de las conexiones de red canceladas se restauran después de que la instalación de la aplicación se complete.

Paso 9. Instalación de la aplicación

La instalación de la aplicación lleva algún tiempo. Espere hasta que se complete.

Si está actualizando una versión anterior de la aplicación, este paso también incluye la configuración de la migración y eliminación de la versión anterior de la aplicación.

Después de que finalice la instalación de Kaspersky Endpoint Security, se inicia el [Asistente de configuración inicial](#).

Instalación de la aplicación desde la línea de comandos

Kaspersky Endpoint Security se puede instalar desde la línea de comandos en una de las siguientes formas:

- En modo interactivo, mediante el Asistente de instalación de la aplicación.
- En modo silencioso. Una vez que la instalación se inicie en el modo silencioso, su participación en el proceso de instalación ya no se requiere. Para instalar la aplicación en modo silencioso, utilice las claves /s y /qn.

Para instalar la aplicación o actualizar la versión de la aplicación:

1. Ejecute el intérprete de la línea de comandos (cmd.exe) como administrador.
2. Vaya a la carpeta donde está ubicado el paquete de distribución de Kaspersky Endpoint Security.
3. Ejecute el siguiente comando:

```
setup kes.exe/pEULA=1/pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1|0] [/pADDLOCAL=  
<componente>] [/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/pKLLOGIN=<nombre  
de usuario> /pKLPASSWD=<contraseña> /pKLPASSWDAREA=<alcance de la contraseña>]  
[/pENABLETRACES=1|0 /pTRACESLEVEL=<nivel de seguimiento>]/s
```

o bien

```
Msiexec /i <nombre del kit de distribución> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]  
[ALLOWREBOOT=1|0] [ADDLOCAL=<componente>] [SKIPPRODUCTCHECK=1|0]  
[SKIPPRODUCTUNINSTALL=1|0] [KLLOGIN=<nombre de usuario> KLPASSWD=<contraseña>  
KLPASSWDAREA=<alcance de la contraseña>] [ENABLETRACES=1|0 TRACESLEVEL=<nivel de  
seguimiento>] /qn
```

EULA	Aceptación o rechazo de los términos del Contrato de licencia de usuario final. Valores disponibles: <ul style="list-style-type: none">• 1: aceptación de las condiciones del Contrato de licencia de usuario final.• 0: rechazo de las condiciones del Contrato de licencia de usuario final.
------	---

	<p>El contenido del Contrato de licencia se incluye en el kit de distribución de Kaspersky Endpoint Security. Se requiere la aceptación de los términos del Contrato de licencia de usuario final para instalar la aplicación o actualizar la versión de esta.</p>
PRIVACYPOLICY	<p>Aceptación o rechazo de la Política de privacidad. Valores disponibles:</p> <ul style="list-style-type: none"> • 1: aceptación de la Política de privacidad. • 0: rechazo de la Política de privacidad. <p>El texto de la Política de privacidad se incluye en el Kit de distribución de Kaspersky Endpoint Security. Para instalar la aplicación o actualizar su versión, debe aceptar la Política de privacidad.</p>
KSN	<p>Aceptación o rechazo de la participación en Kaspersky Security Network (KSN). Si no se establece ningún valor para este parámetro, Kaspersky Endpoint Security solicitará la confirmación de su consentimiento o el rechazo de la participación en KSN cuando se inicie Kaspersky Endpoint Security por primera vez. Valores disponibles:</p> <ul style="list-style-type: none"> • 1: aceptación de la participación en KSN. • 0: rechazo de la participación en KSN (valor predeterminado). <p>El paquete de distribución de Kaspersky Endpoint Security se optimiza para su uso con Kaspersky Security Network. Si optara por no participar en Kaspersky Security Network, debería actualizar Kaspersky Endpoint Security inmediatamente después de que la instalación se haya completado.</p>
ALLOWREBOOT=1	<p>Reinicio automático del equipo, si es necesario después de la instalación o la actualización de la aplicación. Si no se establece ningún valor para este parámetro, se bloquea el reinicio automático del equipo.</p> <p>Al instalar Kaspersky Endpoint Security no es necesario reiniciar el equipo. El reinicio es necesario solo si antes de la instalación es necesario eliminar aplicaciones incompatibles. El reinicio también puede ser necesario al actualizar la versión de la aplicación.</p>
ADDLOCAL	<p>Seleccione los componentes adicionales para la instalación. De forma predeterminada, se seleccionan todos los componentes de la aplicación para la instalación, a excepción de los siguientes: Prevención de ataques BadUSB, cifrado de archivos, cifrado de disco completo, Administración de BitLocker y Sensor de Endpoint de KATA. Valores disponibles:</p> <ul style="list-style-type: none"> • MSBitLockerFeature. Se instala el componente Administrador de BitLocker. • AntiAPTFeature. Se instala el componente Sensor de endpoint de KATA.
SKIPPRODUCTCHECK=1	<p>Desactivación de la comprobación de software no compatible. La lista de software no compatible está disponible en el archivo incompatible.txt que se incluye en el kit de distribución. Si no se establece ningún valor para este parámetro y se detecta software no compatible, la instalación de Kaspersky Endpoint Security finalizará.</p>
SKIPPRODUCTUNINSTALL=1	<p>Desactivación de la eliminación automática del software no compatible detectado. Si no se establece ningún valor para este parámetro, Kaspersky Endpoint Security intentará eliminar el software no compatible.</p>

KLLOGIN	<p>Configure el nombre de usuario para acceder a las funciones y ajustes de Kaspersky Endpoint Security (el componente Protección con contraseña). El nombre de usuario se configura a la par de los parámetros KLPASSWD y KLPASSWDAREA. El nombre de usuario predeterminado es KLAdmin.</p>
KLPASSWD	<p>Especifique una contraseña para acceder a las funciones y ajustes de Kaspersky Endpoint Security (la contraseña se especifica junto con los parámetros KLLOGIN y KLPASSWDAREA).</p> <p>Si especificó una contraseña, pero no especificó un nombre de usuario con el parámetro KLLOGIN, se utiliza de forma predeterminada el nombre de usuario KLAdmin.</p>
KLPASSWDAREA	<p>Especifique el alcance de la contraseña para acceder a Kaspersky Endpoint Security. Cuando un usuario intenta realizar una acción que está dentro de este alcance, Kaspersky Endpoint Security solicita las credenciales de la cuenta del usuario (parámetros KLLOGIN y KLPASSWD). Si necesita especificar más de un valor, use el carácter " ; ". Valores disponibles:</p> <ul style="list-style-type: none"> • SET: modificar la configuración de la aplicación. • EXIT: cerrar la aplicación. • DISPROTECT: desactivar componentes de protección y detener tareas de análisis. • DISPOLICY: desactivar la directiva de Kaspersky Security Center. • UNINST: eliminar la aplicación del equipo. • DISCTRL: desactivar componentes de control. • REMOVELIC: eliminar la clave. • REPORTS: consultar informes.
ENABLETRACES	<p>Habilitar o deshabilitar el seguimiento de la aplicación. Una vez que Kaspersky Endpoint Security se inicia, los archivos de rastreo se guardan en la carpeta %ProgramData%/Kaspersky Lab. Valores disponibles:</p> <ul style="list-style-type: none"> • 1: la función de seguimiento de la aplicación está activada. • 0: la función de seguimiento de la aplicación está desactivada (valor predeterminado).
TRACESLEVEL	<p>Nivel de detalle del seguimiento. Valores disponibles:</p> <ul style="list-style-type: none"> • 100 (crítico). Solo los mensajes de error críticos. • 200 (alto). Mensajes sobre todos los errores, incluidos los errores graves. • 300 (diagnóstico). Mensajes sobre todos los errores y una selección de mensajes que contienen advertencias. • 400 (importante). Todas las advertencias y mensajes sobre errores normales y críticos, y una selección de mensajes que contienen

información adicional.

- 500 (normal). Todos advertencias y mensajes sobre errores normales y críticos, y también, mensajes con información detallada acerca del funcionamiento de la aplicación en modo normal (valor predeterminado).
- 600 (bajo). Todos los mensajes posibles.

Ejemplo:

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /s
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1 KLLOGIN=Admin KLPASSWD=Password KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
```

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Después de que se instala la aplicación, Kaspersky Endpoint Security activa la licencia de prueba a menos que haya indicado un código de activación en el [archivo setup.ini](#). La licencia de evaluación suele durar poco tiempo. Cuando finaliza la licencia de evaluación, se desactivan todas las funciones de Kaspersky Endpoint Security. Para seguir utilizando la aplicación, debe [activar una licencia comercial](#).

Al instalar la aplicación o actualizar la versión de aplicación en el modo silencioso, se admite el uso de los archivos siguientes:

- [setup.ini](#): los parámetros generales para la instalación de la aplicación
- [Install.cfg](#): configuración local de Kaspersky Endpoint Security
- setup.reg: claves del registro

Las claves del registro del archivo setup.reg se escriben en el registro sólo si el valor `setup.reg` está establecido para el parámetro `SetupReg` en el archivo setup.ini. El archivo setup.reg es generado por los expertos de Kaspersky. No se recomienda modificar el contenido de este archivo.

Para aplicar la configuración de los archivos setup.ini, install.cfg, y setup.reg, coloque estos archivos en la carpeta que contiene el paquete de distribución de Kaspersky Endpoint Security.

Instalando remotamente la aplicación usando System Center Configuration Manager

Estas instrucciones se aplican a System Center Configuration Manager 2012 R2.

Para una aplicación de forma remota mediante System Center Configuration Manager:

1. Abra la consola de Configuration Manager.

2. En la parte derecha de la consola, en la sección **Administración de aplicaciones**, seleccione **Paquetes**.

3. En la parte superior de la consola del panel de control, haga clic en el botón **Crear paquete**.

Esto inicia el *Asistente de nuevo paquete y aplicación*.

4. En el Asistente de nuevo paquete y aplicación:

a. En la sección **Paquete**:

- En el campo **Nombre**, introduzca el nombre del paquete de instalación.
- En el campo **Carpeta de origen**, especifique la ruta a la carpeta que contiene el kit de distribución de Kaspersky Endpoint Security.

b. En la sección **Tipo de aplicación**, seleccione la opción **Aplicación estándar**.

c. En la sección **Aplicación estándar**:

- En el campo **Nombre**, introduzca el nombre único para el paquete de instalación (por ejemplo, el nombre de la aplicación que incluye la versión).
- En el campo **Línea de comandos**, especifique las opciones de instalación de Kaspersky Endpoint Security en la línea de comandos.
- Haga clic en el botón **Examinar** para especificar la ruta al archivo ejecutable de la aplicación.
- Asegúrese de que la lista **Modo de ejecución** tenga seleccionado el elemento **Ejecutar con derechos de administrador**.

d. En la sección **Requisitos**:

- Seleccione la casilla de verificación **Iniciar primero otra aplicación** si desea que se inicie una aplicación diferente antes de instalar Kaspersky Endpoint Security.

Seleccione la aplicación de la lista desplegable **Aplicación** o especifique la ruta al archivo ejecutable de esta aplicación haciendo clic en el botón **Examinar**.

- Seleccione la opción **Esta aplicación solo se puede iniciar en las plataformas especificadas** en la sección **Requisitos de plataforma** si desea que la aplicación solo se instale en los sistemas operativos especificados.

En la siguiente lista, seleccione las casillas de verificación que hay junto a los sistemas operativos en los cuales se instalará Kaspersky Endpoint Security.

Este paso es opcional.

e. En la sección **Resumen**, compruebe todos los valores de la configuración que se han introducido y haga clic en **Siguiente**.

El paquete de instalación creado aparecerá en la sección **Paquetes** de la lista de paquetes de instalación disponibles.

5. En el menú contextual del paquete de instalación, seleccione **Implementar**.

Esto inicia el *Asistente de implementación*.

6. En el Asistente de implementación:

a. En la sección **General**:

- En el campo **Software**, introduzca el nombre único del paquete de instalación o seleccione el paquete de instalación de la lista haciendo clic en el botón **Examinar**.
- En el campo **Colección**, introduzca el nombre de la colección de equipos en los cuales se instalará la aplicación, o bien seleccione la colección haciendo clic en el botón **Examinar**.

b. En la sección **Contiene**, agregue puntos de distribución (si desea obtener más información, consulte la documentación de ayuda para System Center Configuration Manager).

c. Si es necesario, especifique los valores de otra configuración en el Asistente de implementación. Estos ajustes son opcionales para la instalación remota de Kaspersky Endpoint Security.

d. En la sección **Resumen**, compruebe todos los valores de la configuración que se han introducido y haga clic en **Siguiente**.

Después de que finalice el Asistente de implementación, se creará una tarea para la instalación remota de Kaspersky Endpoint Security.

Descripción de la configuración de instalación del archivo setup.ini

El archivo setup.ini se utiliza al instalar la aplicación desde la línea de comandos o al utilizar del Editor de directivas de grupo de Microsoft Windows. Para aplicar la configuración del archivo setup.ini, coloque estos archivos en la carpeta que contiene el paquete de distribución de Kaspersky Endpoint Security.

El archivo setup.ini contiene las siguientes secciones:

- [Setup]: opciones generales de instalación de la aplicación:
- [Componentes]: selección de los componentes de la aplicación que se van a instalar. Si no se especifica ningún componente, se instalarán todos los componentes que estén disponibles en el sistema operativo. Antivirus de archivos es un componente obligatorio y se instala en el equipo sin tener en cuenta qué configuración se indicó en esta sección.
- [Tareas]: selección de tareas que se incluirán en la lista de tareas de Kaspersky Endpoint Security. Si no se especifica la tarea, se incluirán todas las tareas de la lista de tareas de Kaspersky Endpoint Security.

Las alternativas al valor 1 son los valores yes, on, enable y enabled.

Las alternativas al valor 0 son los valores no, off, disable y disabled.

Configuración del archivo setup.ini

Sección	Parámetro	Descripción
[Instalación]	InstallDir	Ruta a la carpeta de instalación de la aplicación.
	ActivationCode	Código de activación de Kaspersky Endpoint Security.
	Eula	Aceptación o rechazo de los términos del Contrato de licencia de usuario final. Valores

		<p>disponibles:</p> <ul style="list-style-type: none"> • 1: aceptación de las condiciones del Contrato de licencia de usuario final. • 0: rechazo de las condiciones del Contrato de licencia de usuario final. El contenido del Contrato de licencia se incluye en el kit de distribución de Kaspersky Endpoint Security. Se requiere la aceptación de los términos del Contrato de licencia de usuario final para instalar la aplicación o actualizar la versión de esta.
	PrivacyPolicy	<p>Aceptación o rechazo de la Política de privacidad. Valores disponibles:</p> <ul style="list-style-type: none"> • 1: aceptación de la Política de privacidad. • 0: rechazo de la Política de privacidad. El texto de la Política de privacidad se incluye en el Kit de distribución de Kaspersky Endpoint Security. Para instalar la aplicación o actualizar su versión, debe aceptar la Política de privacidad.
	KSN	<p>Aceptación o rechazo de la participación en Kaspersky Security Network (KSN). Si no se establece ningún valor para este parámetro, Kaspersky Endpoint Security solicitará la confirmación de su consentimiento o el rechazo de la participación en KSN cuando se inicie Kaspersky Endpoint Security por primera vez. Valores disponibles:</p> <ul style="list-style-type: none"> • 1: aceptación de la participación en KSN. • 0: rechazo de la participación en KSN (valor predeterminado). El paquete de distribución de Kaspersky Endpoint Security se optimiza para su uso con Kaspersky Security Network. Si optara por no participar en Kaspersky Security Network, debería actualizar Kaspersky Endpoint Security inmediatamente después de que la instalación se haya completado.
	Login	<p>Configure el nombre de usuario para acceder a las funciones y ajustes de Kaspersky Endpoint Security (el componente Protección con contraseña). El nombre de usuario se configura junto con los ajustes Password y PasswordArea. El nombre de usuario predeterminado es KLAdmin.</p>
	Contraseña	<p>Especifique una contraseña para acceder a las funciones y ajustes de Kaspersky Endpoint Security (la contraseña se especifica junto con los parámetros Login y PasswordArea).</p>

		Si especificó una contraseña, pero no especificó un nombre de usuario con el parámetro Nombre de usuario, se utiliza de forma predeterminada el nombre de usuario KAdmin.
	PasswordArea	<p>Especifique el alcance de la contraseña para acceder a Kaspersky Endpoint Security. Cuando un usuario intenta realizar una acción que está dentro de este alcance, Kaspersky Endpoint Security solicita las credenciales de la cuenta del usuario (parámetros Login y Contraseña). Si necesita especificar más de un valor, use el carácter ";".</p> <p>Valores disponibles:</p> <ul style="list-style-type: none"> • SET: modificar la configuración de la aplicación. • EXIT: cerrar la aplicación. • DISPROTECT: desactivar componentes de protección y detener tareas de análisis. • DISPOLICY: desactivar la directiva de Kaspersky Security Center. • UNINST: eliminar la aplicación del equipo. • DISCTRL: desactivar componentes de control. • REMOVELIC: eliminar la clave. • REPORTS: consultar informes.
	SelfProtection	<p>Activación o desactivación del mecanismo que protege la instalación de la aplicación. Valores disponibles:</p> <ul style="list-style-type: none"> • 1: se activa el mecanismo de protección de la instalación de la aplicación. • 0: se desactiva el mecanismo de protección de la instalación de la aplicación. Puede desactivar la protección de la instalación. La protección de la instalación incluye protección contra la sustitución del paquete de distribución por malware, el bloqueo del acceso a la carpeta de instalación de Kaspersky Endpoint Security y el bloqueo del acceso al subárbol del registro del sistema que contiene las claves de la aplicación. Sin embargo, si no se puede instalar la aplicación (por ejemplo, cuando se realiza la instalación remota con la ayuda del Escritorio remoto de Windows), se aconseja que desactive la protección del proceso de instalación.
	Reboot=1	Reinicio automático del equipo, si es necesario después de la instalación o la actualización de la aplicación. Si no se establece ningún valor para

		<p>este parámetro, se bloquea el reinicio automático del equipo.</p> <p>Al instalar Kaspersky Endpoint Security no es necesario reiniciar el equipo. El reinicio es necesario solo si antes de la instalación es necesario eliminar aplicaciones incompatibles. El reinicio también puede ser necesario al actualizar la versión de la aplicación.</p>
	AddEnvironment	<p>Complementa la variable del sistema %PATH% con la ruta de los archivos ejecutables que se ubican en la carpeta de instalación de Kaspersky Endpoint Security. Valores disponibles:</p> <ul style="list-style-type: none"> • 1: la variable del sistema %PATH% se complementa con la ruta de los archivos ejecutables que se ubican en la carpeta de instalación de Kaspersky Endpoint Security. • 0: la variable del sistema %PATH% no se complementa con la ruta de los archivos ejecutables que se ubican en la carpeta de instalación de Kaspersky Endpoint Security.
	AMPPL	<p>Activar o desactivar la protección del servicio de seguridad de los puntos finales de Kaspersky usando la tecnología AM-PPL (Antimalware Protected Process Light). Valores disponibles:</p> <ul style="list-style-type: none"> • 1: el servicio de Kaspersky Endpoint Security se protege con la tecnología AM-PPL. • 0: el servicio de Kaspersky Endpoint Security no se protege con la tecnología AM-PPL.
	SetupReg	<p>Permite que se graben en el Registro las claves del archivo setup.reg. SetupReg: valor del parámetro setup.reg.</p>
	EnableTraces	<p>Habilitar o deshabilitar el seguimiento de la instalación de la aplicación. Kaspersky Endpoint Security guarda los archivos de rastreo en la carpeta %ProgramData%/Kaspersky Lab. Valores disponibles:</p> <ul style="list-style-type: none"> • 1: el seguimiento de la instalación de la aplicación está habilitado. • 0: el seguimiento de la instalación de la aplicación está deshabilitado.(valor predeterminado).
	TracesLevel	<p>Nivel de detalle del seguimiento. Valores disponibles:</p> <ul style="list-style-type: none"> • 100 (crítico). Solo los mensajes de error críticos.

		<ul style="list-style-type: none"> • 200 (alto). Mensajes sobre todos los errores, incluidos los errores graves. • 300 (diagnóstico). Mensajes sobre todos los errores y una selección de mensajes que contienen advertencias. • 400 (importante). Todas las advertencias y mensajes sobre errores normales y críticos, y una selección de mensajes que contienen información adicional. • 500 (normal). Todos advertencias y mensajes sobre errores normales y críticos, y también, mensajes con información detallada acerca del funcionamiento de la aplicación en modo normal (valor predeterminado). • 600 (bajo). Todos los mensajes posibles.
[Componentes]	ALL	Instalar todos los componentes. Si se especifica el valor del parámetro 1, todos los componentes se instalarán sin tener en cuenta la configuración de la instalación de componentes concretos.
	MailAntiVirus	Antivirus del correo.
	IMAntiVirus	Antivirus para chat.
	WebAntiVirus	Antivirus Internet.
	ApplicationPrivilegeControl	Control de actividad de aplicaciones.
	SystemWatcher	System Watcher.
	Firewall	Firewall.
	NetworkAttackBlocker	Prevención de intrusiones.
	WebControl	Control web.
	DeviceControl	Control de dispositivos.
	ApplicationStartupControl	Control de inicio de aplicaciones.
	FileEncryption	Bibliotecas de cifrado de archivos.
	DiskEncryption	Bibliotecas de cifrado de disco completo.
	VulnerabilityAssessment	Control de vulnerabilidades.
	KeyboardAuthorization	Prevención de ataques de BadUSB.
	AntiAPT	Sensor de Endpoint de KATA.
	MSBitLocker	Administrador de Microsoft BitLocker.
	AdminKitConnector	<p>Conector del agente de red para administrar de forma remota la aplicación a través de Kaspersky Security Center. Valores disponibles:</p> <ul style="list-style-type: none"> • 1: se instala el Conector del agente de red. • 0: no se instala el Conector del agente de red.

[Tareas]	ScanMyComputer	Tarea de Análisis completo. Valores disponibles: <ul style="list-style-type: none"> • 1: se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security. • 0: no se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security.
	ScanCritical	Tarea de Análisis de áreas críticas. Valores disponibles: <ul style="list-style-type: none"> • 1: se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security. • 0: no se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security.
	Updater	Tarea de actualización. Valores disponibles: <ul style="list-style-type: none"> • 1: se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security. • 0: no se incluye la tarea en la lista de tareas de Kaspersky Endpoint Security.

Asistente de configuración inicial

El Asistente de configuración inicial de Kaspersky Endpoint Security se inicia al final del proceso de instalación de la aplicación. El Asistente de configuración inicial permite activar la aplicación y recopila la información sobre las aplicaciones que se incluyen en el sistema operativo. Estas aplicaciones se agregan a la lista de aplicaciones de confianza cuyas acciones dentro del sistema operativo no están sujetas a ninguna restricción.

La interfaz del Asistente de configuración inicial consta de una secuencia de páginas (pasos). Puede navegar por las páginas del Asistente de configuración inicial utilizando los botones **Atrás** y **Siguiente**. Para completar el procedimiento del Asistente de configuración inicial, haga clic en **Terminar**. Para interrumpir el Asistente de configuración inicial en cualquier momento, haga clic en **Cancelar**.

Si se interrumpe el Asistente de configuración inicial por algún motivo, no se guardará la configuración que ya se haya especificado. La próxima vez que intente utilizar la aplicación, el Asistente de configuración inicial volverá a iniciar y tendrá que configurar los parámetros desde cero.

Activación de la aplicación

La aplicación debe activarse en un equipo con la fecha y la hora del sistema actuales. Si la fecha y la hora del sistema se cambian después de la activación de la aplicación, la clave no puede usarse. La aplicación cambia a un modo de funcionamiento sin actualizaciones y Servicio de reputación de KSN no está disponible. La clave solo puede volver a utilizarse mediante la reinstalación del sistema operativo.

En este punto, seleccione una de las siguientes opciones de activación de Kaspersky Endpoint Security:

- **Activar con un código de activación.** Para activar la aplicación mediante un código de activación, seleccione esta opción e introduzca el [código de activación](#).
- **Activar con un archivo llave.** Seleccione esta opción para activar la aplicación mediante un archivo llave.
- **Activar la versión de evaluación.** Para activar la versión de evaluación de la aplicación, seleccione esta opción. El usuario puede utilizar la versión completa de la aplicación durante el período que establece la licencia de la versión de evaluación de la aplicación. Cuando finaliza la licencia, se bloquea la funcionalidad de la aplicación y no puede volver a activar la versión de evaluación.
- **Activar más tarde.** Seleccione esta opción si desea omitir la activación de Kaspersky Endpoint Security. El usuario solo dispondrá de los componentes Antivirus de archivos y Firewall. El usuario solo podrá actualizar las bases de datos antivirus y los módulos de Kaspersky Endpoint Security después de la instalación. La opción **Activar más tarde** solo está disponible la primera vez que inicia el Asistente de configuración inicial, inmediatamente después de instalar la aplicación.

Se requiere conexión a Internet para activar la versión de evaluación de la aplicación o para activar la aplicación con un código de activación.

Para continuar con el Asistente de configuración inicial, seleccione una opción de activación y haga clic en el botón **Siguiente**. Para interrumpir el Asistente de configuración inicial, haga clic en el botón **Cancelar**.

Activar con un código de activación

Este paso está disponible solo cuando activa la aplicación mediante un código de activación. Este paso se omite cuando activa la versión de evaluación de la aplicación o cuando activa la aplicación por medio de un archivo llave.

Durante este paso, Kaspersky Endpoint Security envía datos al servidor de activación para comprobar el código de activación introducido:

- Si la verificación del código de activación es correcta, el Asistente de configuración inicial pasa a la siguiente ventana.
- Si la comprobación del código de activación falla, aparece un mensaje correspondiente. En este caso, debería solicitar asistencia al proveedor de software que le vendió la licencia de Kaspersky Endpoint Security.
- Si se supera el número de activaciones con el código de activación, aparecerá la notificación correspondiente. Se interrumpe el Asistente de configuración inicial y la aplicación le sugiere que se ponga en contacto con el Soporte técnico de Kaspersky.

Para volver al paso anterior del Asistente de configuración inicial, haga clic en el botón **Atrás**. Para interrumpir el Asistente de configuración inicial, haga clic en el botón **Cancelar**.

Activar con un archivo clave

Este paso está disponible solo cuando activa la aplicación por medio de un archivo llave.

En este punto, debe especificar la ruta del archivo llave. Para ello, haga clic en el botón **Examinar** y seleccione un archivo llave que presente el formato <ID de archivo>.key.

Una vez que haya seleccionado el archivo llave, se muestra la siguiente información en la parte inferior de la ventana:

- Clave
- Tipo de licencia (comercial o de evaluación) y número de equipos que cubre esta licencia
- Fecha de la activación de la aplicación en el equipo
- Fecha de caducidad de la licencia
- Funcionalidad de la aplicación disponible según la licencia
- Notificaciones sobre problemas importantes, en caso de que existan. Por ejemplo, *Lista negra de claves dañada*.

Para volver al paso anterior del Asistente de configuración inicial, haga clic en el botón **Atrás**. Para seguir con el Asistente de configuración inicial, haga clic en el botón **Siguiente**. Para interrumpir el Asistente de configuración inicial, haga clic en el botón **Cancelar**.

Selección de funciones que activar

Este paso está disponible solo cuando activa la versión de evaluación de la aplicación.

En este paso, puede seleccionar la funcionalidad que estará disponible cuando se active la aplicación:

- **Instalación básica.** Si se selecciona esta opción, solo estarán disponibles después de la activación de la aplicación los componentes de protección, Control de actividad de aplicaciones y Control de vulnerabilidades.
- **Instalación estándar.** Si se selecciona esta opción, solo los componentes de protección y control de la aplicación estarán disponibles después de la activación.
- **Instalación completa.** Si se selecciona esta opción, todos los componentes instalados de la aplicación, incluida la funcionalidad de cifrado, estarán disponibles después de la activación de la aplicación.

Si seleccionó más componentes aparte de los permisos de licencia adquiridos durante la instalación, después de la activación de la aplicación, los componentes que no estén disponibles según la licencia se instalarán, pero no estarán operativos. Si la licencia adquirida permite el uso de más componentes de los actualmente instalados, después de que se active la aplicación los componentes que no se han instalado se muestran en la sección **Licencia**.

La instalación estándar está seleccionada de forma predeterminada.

Para volver al paso anterior del Asistente de configuración inicial, haga clic en el botón **Atrás**. Para seguir con el Asistente de configuración inicial, haga clic en el botón **Siguiente**. Para interrumpir el Asistente de configuración inicial, haga clic en el botón **Cancelar**.

Completar la activación

Durante este paso, el Asistente de configuración inicial le informa sobre el éxito de la activación de Kaspersky Endpoint Security. Se proporcionará la siguiente información acerca de la licencia:

- Tipo de licencia (comercial o de evaluación) y número de equipos que cubre esta licencia
- Fecha de caducidad de la licencia
- Funcionalidad de la aplicación disponible según la licencia

Para seguir con el Asistente de configuración inicial, haga clic en el botón **Siguiente**. Para interrumpir el Asistente de configuración inicial, haga clic en el botón **Cancelar**.

Análisis del sistema operativo

Durante este paso, se recopila la información de las aplicaciones que están incluidas en el sistema operativo. Estas aplicaciones se agregan a la lista de aplicaciones de confianza cuyas acciones dentro del sistema operativo no están sujetas a ninguna restricción.

Se analizan otras aplicaciones cuando se ha iniciado por primera vez la instalación de Kaspersky Endpoint Security.

Para interrumpir el Asistente de configuración inicial, haga clic en el botón **Cancelar**.

Finalización de la configuración inicial de la aplicación

La ventana de finalización del Asistente de configuración inicial contiene información sobre la finalización del proceso de instalación de Kaspersky Endpoint Security.

Si desea iniciar Kaspersky Endpoint Security, haga clic en el botón **Finalizar**.

Si desea salir del Asistente de configuración inicial sin iniciar Kaspersky Endpoint Security, desactive la casilla de verificación **Iniciar Kaspersky Endpoint Security 10 para Windows** y haga clic en **Finalizar**.

Declaración de Kaspersky Security Network

Durante este paso, se le invita a participar en Kaspersky Security Network.

Revise la declaración de Kaspersky Security Network:

- Si acepta todos los términos, seleccione la opción **Acepto los términos de participación en Kaspersky Security Network** en la ventana del Asistente de configuración inicial.
- Si no acepta los términos de participación en Kaspersky Security Network, seleccione la opción **No acepto los términos de participación en Kaspersky Security Network** en la ventana del Asistente de configuración inicial.

Para continuar el Asistente de configuración inicial, haga clic en **Aceptar**.

Acerca de las formas de actualizar una versión antigua de la aplicación

Para actualizar una versión anterior de la aplicación a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, descifre todos los discos duros cifrados.

Puede actualizar las siguientes aplicaciones a Kaspersky Endpoint Security 10 Service Pack 2 para Windows:

- Kaspersky Anti-Virus 6.0 para Windows Workstations MP4 CF1 (compilación 6.0.4.1424)/MP4 CF2 (compilación 6.0.4.1611)
- Kaspersky Anti-Virus 6.0 para Windows Servers MP4 (compilación 6.0.4.1424)/MP4 CF2 (compilación 6.0.4.1611)
- Kaspersky Endpoint Security 10 Service Pack 1 para Windows (compilación 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 para Windows (compilación 10.2.2.10535 [MR1])
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 para Windows (compilación 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 para Windows (compilación 10.2.5.3201).

Cuando alguna de las aplicaciones anteriormente enumeradas se actualiza a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, no se transfieren los contenidos de Cuarentena y Respaldo.

Puede actualizar la versión antigua de la aplicación de la siguiente forma:

- De forma local en modo interactivo, mediante el Asistente de instalación de la aplicación.
- De forma local en modo no interactivo, desde la [línea de comandos](#)
- De forma remota, mediante el paquete de software de Kaspersky Security Center (consulte la *Guía de implementación de Kaspersky Security Center*).
- De forma remota, mediante el Editor de directivas de grupo de Microsoft Windows (consulte los archivos de ayuda del sistema operativo).

Cuando se actualiza una versión anterior de la aplicación a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, no es necesario eliminar la versión anterior de la aplicación. Recomendamos que cierre todas las aplicaciones en funcionamiento antes de actualizar a una versión anterior de la aplicación.

Eliminación de la aplicación

Esta sección describe cómo eliminar Kaspersky Endpoint Security del equipo.

Acerca de las formas de eliminar la aplicación

La eliminación de Kaspersky Endpoint Security deja al equipo y a los datos del usuario desprotegidos frente a las amenazas.

Kaspersky Endpoint Security se puede eliminar desde el equipo de varias formas:

- De forma local en modo interactivo, mediante el [Asistente de instalación](#)
- De forma local en modo no interactivo, desde la [línea de comandos](#)
- De forma remota, mediante el paquete de software de Kaspersky Security Center (consulte la *Guía de implementación de Kaspersky Security Center* para obtener más detalles).
- De forma remota, mediante el Editor de directivas de grupo de Microsoft Windows (consulte los archivos de ayuda del sistema operativo).

Eliminación de la aplicación mediante el Asistente de instalación

Para eliminar Kaspersky Endpoint Security mediante el Asistente de instalación:

1. En el menú **Inicio**, seleccione **Aplicaciones** → **Kaspersky Endpoint Security 10 para Windows** → **Modificar, reparar o quitar**.
Se iniciará el Asistente de instalación.
2. En la ventana **Modificar, reparar o eliminar aplicación** del Asistente de instalación, haga clic en el botón **Eliminar**.
3. Siga las instrucciones del Asistente de instalación.

Paso 1. Almacenamiento de los datos de la aplicación para su uso posterior

Durante este paso, puede especificar cuáles de los datos utilizados por la aplicación desea mantener para usarlos más adelante, durante la siguiente instalación de la aplicación (por ejemplo, al instalar una versión más reciente). Si no especifica ningún dato, la aplicación se eliminará por completo.

Con el fin de guardar los datos de la aplicación para su uso posterior:

Seleccione las casillas de verificación que hay junto a los tipos de datos que desea guardar:

- **Datos de activación:** estos datos eliminan la necesidad de activar las aplicaciones que instale en el futuro. Se activarán de forma automática con la licencia actual, siempre y cuando dicha licencia no haya caducado antes de la instalación.
- **Archivos de Respaldo y Cuarentena:** archivos que la aplicación analiza y ubica en Respaldo o Cuarentena.

Se puede acceder a los archivos de Respaldo y Cuarentena que se han guardado después de eliminar la aplicación únicamente desde la misma versión de la aplicación que se utilizó para guardar los archivos.

Si tiene pensado usar objetos de Respaldo y Cuarentena después de eliminar la aplicación, antes debe restaurar los objetos desde sus almacenes. Sin embargo, los expertos de Kaspersky no recomiendan la restauración de archivos desde Respaldo y Cuarentena, pues pueden dañar el equipo.

- **Parámetros operativos de la aplicación:** Parámetros de la aplicación que se seleccionan durante la configuración de la aplicación.
- **Almacenamiento local de las claves de cifrado:** datos que proporcionan acceso directo a los archivos y dispositivos que se cifraron antes de la eliminación de la aplicación. Se puede acceder directamente a las unidades y los archivos cifrados cuando se vuelva a instalar la aplicación con la funcionalidad de cifrado. Esta casilla de verificación está seleccionada de forma predeterminada.

Para seguir con el Asistente de instalación, haga clic en el botón **Siguiente**. Para interrumpir el Asistente de instalación, haga clic en el botón **Cancelar**.

Paso 2. Confirmación de la eliminación de la aplicación

Puesto que la eliminación de la aplicación pone en peligro la seguridad de su equipo, se le solicita que confirme que desea eliminar la aplicación. Para ello, haga clic en el botón **Eliminar**.

Para detener la eliminación de la aplicación en cualquier momento, puede cancelar la operación haciendo clic en **Cancelar**.

Paso 3. Eliminación de la aplicación. Completando eliminación

Durante este paso, el Asistente de instalación elimina la aplicación del equipo. Espere a que se complete la eliminación.

Cuando elimine la aplicación, es posible que su sistema operativo requiera el reinicio del equipo. Si decide no reiniciar de inmediato, el proceso de finalización de la aplicación se pospone hasta que se reinicie el sistema operativo o hasta que el equipo se apague y se vuelva a encender.

Eliminación de la aplicación de la línea de comandos

Puede iniciar el proceso de desinstalación de la aplicación desde la línea de comandos. La desinstalación se realiza en el modo interactivo o silencioso (sin iniciar el Asistente de instalación de la aplicación).

Para iniciar el proceso de desinstalación de la aplicación en el modo interactivo,

escriba en la línea de comandos `setup.exe /x` o `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

Se iniciará el Asistente de instalación. Siga las instrucciones del [Asistente de instalación](#).

Para iniciar el proceso de desinstalación de la aplicación en el modo silencioso,

escriba en la línea de comandos `setup.exe /s /x o msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`.

Esto inicia el proceso de desinstalación de la aplicación en el modo silencioso (sin iniciar el Asistente de instalación).

Si la operación de desinstalación de aplicación está protegida con contraseña, el nombre de usuario y su contraseña correspondiente se deben introducir en la línea de comandos.

Con el fin de eliminar la aplicación desde la línea de comandos en el modo interactivo cuando se han definido el nombre de usuario y la contraseña para la autenticación de la eliminación, modificación o reparación de Kaspersky Endpoint Security:

En la línea de comandos, escriba `setup.exe /pKLLOGIN=<Nombre de usuario> /pKLpasswd=***** /x o`

`msiexec.exe KLLOGIN=<Nombre de usuario> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

Se iniciará el Asistente de instalación. Siga las instrucciones del [Asistente de instalación](#).

Con el fin de eliminar la aplicación desde la línea de comandos en el modo silencioso cuando se han definido el nombre de usuario y la contraseña para la autenticación de la eliminación, modificación o reparación de Kaspersky Endpoint Security:

En la línea de comandos, escriba `setup.exe /pKLLOGIN=<Nombre de usuario> /pKLpasswd=***** /s /x o`

`msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLOGIN=<Nombre de usuario> KLPASSWD=***** /qn`.

Eliminar los objetos y datos que permanecen después de la operación de prueba del Agente de autenticación

Durante la desinstalación de la aplicación, si Kaspersky Endpoint Security detecta objetos y datos que permanecieron en el disco duro del sistema después de la operación de prueba del Agente de autenticación, la desinstalación de aplicación se interrumpe y se hace imposible hasta que esos objetos y datos se eliminan.

Solamente en casos excepcionales, los objetos y los datos pueden permanecer en el disco duro del sistema después de la operación de prueba del Agente de autenticación. Por ejemplo, esto puede suceder si el equipo no se ha reiniciado después de que se aplicara una directiva de Kaspersky Security Center con configuración de cifrado o la aplicación no puede iniciarse después de la operación de prueba del Agente de autenticación.

Existen dos formas de eliminar los objetos y los datos que permanecen en el disco duro del sistema después de la operación de prueba del Agente de autenticación:

- Mediante la directiva de Kaspersky Security Center.
- Mediante Utilidad de restauración.

Para utilizar una directiva de Kaspersky Security Center con el fin de eliminar objetos y datos que permanecieron después de la operación de prueba del Agente de autenticación:

1. Aplique al equipo una directiva de Kaspersky Security Center con la configuración definida para [descifrar](#) todos los discos duros del equipo.

2. Inicie Kaspersky Endpoint Security.

Para usar la Utilidad de restauración con el fin de eliminar objetos y datos que permanecieron después de la operación de prueba del Agente de autenticación:

1. Inicie Utilidad de restauración ejecutando el archivo fdert.exe [creado con Kaspersky Endpoint Security](#) en el equipo con el disco duro del sistema conectado en el que sigue habiendo objetos y datos después de la operación de prueba del agente de autenticación.
2. En la lista desplegable **Seleccionar dispositivo** de la ventana Utilidad de restauración, seleccione el disco duro del sistema con los objetos y datos que desea eliminar.
3. Haga clic en el botón **Analizar**.
4. Haga clic en el botón **Eliminar objetos y datos de AA**.

Esto inicia el proceso de eliminación de objetos y datos que permanecieron después de la operación de prueba del Agente de autenticación.

Tras eliminar los objetos y los datos que permanecían después de la operación de prueba del Agente de autenticación, puede que también deba eliminar la información acerca de la incompatibilidad de la aplicación con el Agente de autenticación.

Para eliminar la información sobre la incompatibilidad de la aplicación con Agente de autenticación,

escriba el comando `avp pbatestreset` en la línea de comandos.

Se deben instalar los componentes de cifrado para que el comando `avp pbatestreset` se ejecute.

Interfaz de la aplicación

Esta sección describe los elementos fundamentales de la interfaz de la aplicación.

Icono de la aplicación en el área de notificaciones de la barra de tareas




Inmediatamente después de la instalación de Kaspersky Endpoint Security, su icono aparece en el área de notificaciones de la barra de tareas de Microsoft Windows.

El icono tiene las siguientes finalidades:

- Indica la actividad de la aplicación.
- Actúa como acceso directo al menú contextual y la ventana principal de la aplicación.

Indicación de la actividad de la aplicación

El icono de la aplicación actúa como indicador de la actividad de la aplicación:

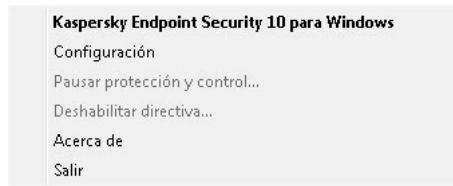
- El icono  indica que todos los componentes de protección de la aplicación están activados.
- El icono  indica que durante el funcionamiento de Kaspersky Endpoint Security se han producido eventos importantes que requieren su atención. Por ejemplo, se ha desactivado Antivirus de archivos o las bases de datos de la aplicación no están actualizadas.
- El icono  indica que se han producido eventos críticos durante el funcionamiento de Kaspersky Endpoint Security. Por ejemplo, un error en el funcionamiento de un componente o daños en las bases de datos de la aplicación.

Menú contextual del icono de la aplicación

El menú contextual del icono de la aplicación contiene los siguientes elementos:

- **Kaspersky Endpoint Security 10 para Windows.** Abre la pestaña **Protección y control** en la ventana principal de la aplicación. La pestaña **Protección y control** permite ajustar el funcionamiento de los componentes y las tareas de la aplicación, así como ver las estadísticas de archivos procesados y amenazas detectadas.
- **Configuración.** Abre la pestaña **Configuración** en la ventana principal de la aplicación. La pestaña **Configuración** permite cambiar la configuración predeterminada de la aplicación.
- **Pausar protección y control/Reanudar protección y control.** Suspende o reanuda temporalmente el funcionamiento de los componentes de protección y control. Este elemento de menú contextual no influye en la tarea de actualización ni en las tareas de análisis, y está disponible solo cuando se desactiva la directiva de Kaspersky Security Center.
- **Deshabilitar directiva/Habilitar directiva.** Deshabilita o habilita la directiva de Kaspersky Security Center. Este elemento de menú contextual está disponible cuando Kaspersky Endpoint Security funciona de acuerdo con una directiva y se ha configurado una contraseña para desactivar la directiva de Kaspersky Security Center.

- **Acerca de.** Este elemento abre una ventana de información con detalles sobre la aplicación.
- **Salir.** Este elemento cierra Kaspersky Endpoint Security. Al hacer clic en este menú contextual, la aplicación se descarga de la RAM del equipo.







Menú contextual del icono de la aplicación




Puede abrir el menú contextual del icono de la aplicación si coloca el puntero sobre este icono en el área de notificaciones de la barra de tareas de Microsoft Windows y hace clic con el botón derecho.

Ventana principal de la aplicación

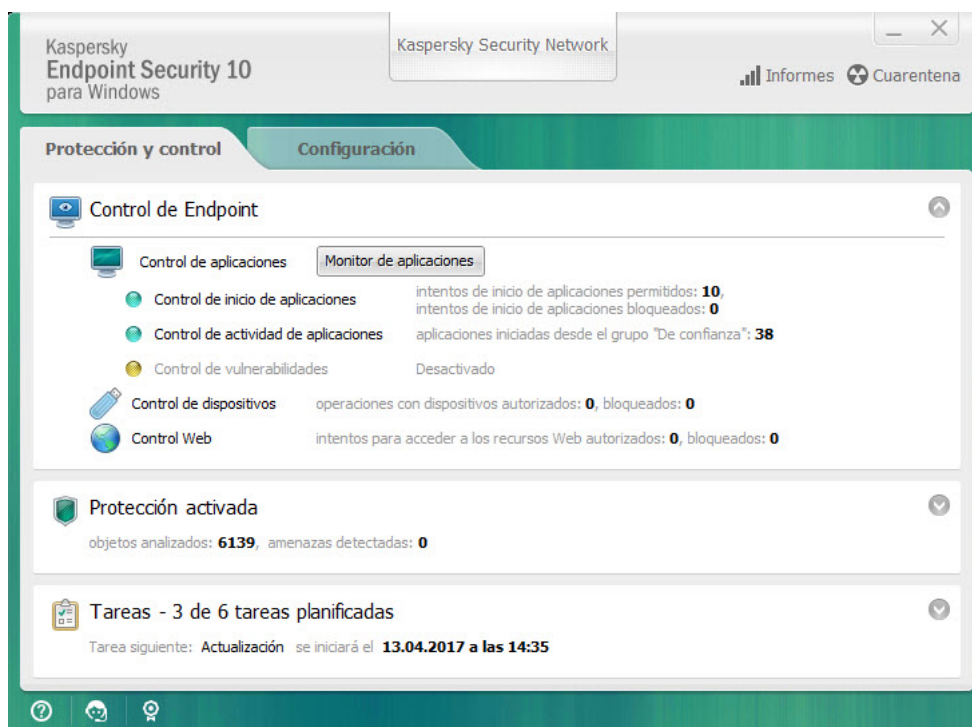
La ventana principal de Kaspersky Endpoint Security contiene elementos de la interfaz que proporcionan acceso a las principales funciones de la aplicación.

La ventana principal de la aplicación está dividida en cuatro partes (consulte la siguiente imagen):

- La parte superior de la ventana contiene los elementos de la interfaz que le permiten ver la siguiente información:
 - Detalles sobre la aplicación
 - Estadísticas de Kaspersky Security Network
 - Lista de archivos sin procesar
 - Lista de vulnerabilidades detectadas
 - Lista de archivos en cuarentena
 - Almacenamiento de copias de archivos infectados que la aplicación ha eliminado
 - Informes sobre eventos que se han producido durante el funcionamiento de la aplicación en general o de sus componentes individuales, o durante la realización de tareas
- La pestaña **Protección y control** permite ajustar el funcionamiento de los componentes y la finalización de las tareas. La pestaña **Protección y control** se muestra al abrir la ventana principal de la aplicación.
- La pestaña **Configuración** permite editar la configuración predeterminada de la aplicación.
- La parte inferior de la ventana contiene los elementos siguientes:
 - **Botón** . Al hacer clic en este botón, accede al sistema de ayuda de Kaspersky Endpoint Security.
 - **Botón** . Al hacer clic en este botón, se abre la ventana **Soporte**, que contiene información sobre el sistema operativo, la versión actual de Kaspersky Endpoint Security y enlaces a recursos de información de Kaspersky.
 - **Botón**  / . Al hacer clic en este botón, se abre la ventana **Licencia**, que contiene información sobre la licencia actual.

- **Botón**  /  /  Al hacer clic en este botón se abre la ventana **Eventos**, que contiene información sobre actualizaciones disponibles y sobre solicitudes para acceder a archivos y dispositivos cifrados.

El botón solo está disponible cuando hay solicitudes de acceso o actualizaciones desinstaladas.



Ventana principal de la aplicación

Para abrir la ventana principal de Kaspersky Endpoint Security, realice una de las siguientes acciones:

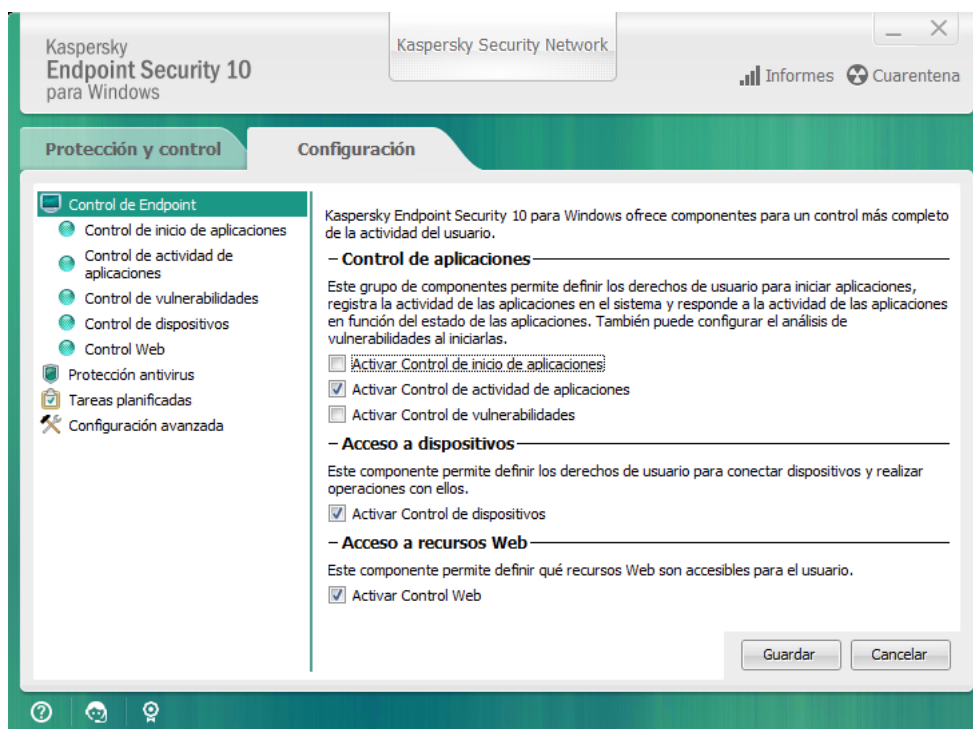
- Haga clic en el icono de la aplicación en el área de notificaciones de la barra de tareas de Microsoft Windows.
- Seleccione **Kaspersky Endpoint Security 10 para Windows** en el [menú contextual del icono de la aplicación](#).

Configurar pestaña Configuración de la aplicación

La pestaña de configuración de Kaspersky Endpoint Security permite configurar los parámetros generales de la aplicación, componentes individuales, informes y almacenes, tareas de análisis, tareas de actualización, tareas de análisis de vulnerabilidades y la comunicación con Kaspersky Security Network.

La pestaña de configuración de la aplicación consta de dos partes (consulte la siguiente figura):

- La parte izquierda contiene componentes de la aplicación, tareas y una sección de configuración avanzada que consta de varios apartados.
- La parte derecha contiene elementos de control que puede utilizar para configurar los ajustes del componente o la tarea seleccionada en la parte izquierda de la ventana, así como la configuración avanzada.



Configurar pestaña Configuración de la aplicación

Para abrir la pestaña de configuración de la aplicación, realice una de las siguientes acciones:

- En la [ventana principal de la aplicación](#), seleccione la pestaña **Configuración**.
- En el [icono del menú contextual de la aplicación](#), seleccione **Configuración**.

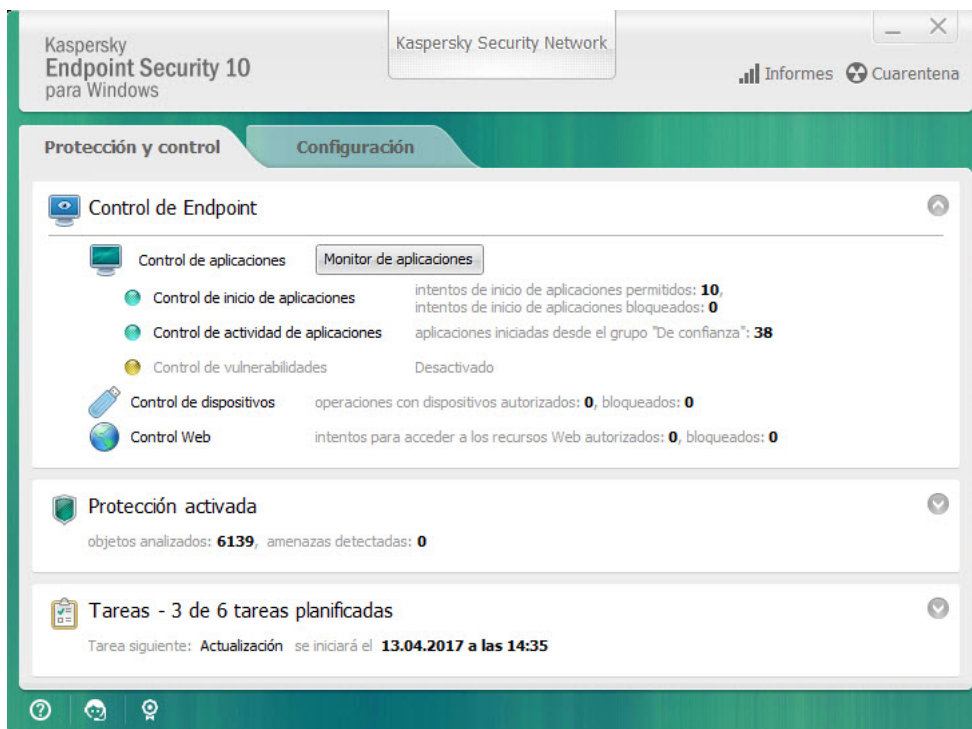
Pestaña Protección y control de aplicaciones

La pestaña Protección y control de Kaspersky Endpoint Security está pensada para proporcionar la información general sobre el rendimiento de todas las tareas y el funcionamiento de todos los componentes de la aplicación. En esta pestaña, también puede regular el funcionamiento de los componentes y el rendimiento de las tareas.

La pestaña Protección y control de aplicaciones consta de tres partes (consulte la siguiente figura):

- La sección **Control de Endpoint** contiene una lista de los componentes de control.
- La sección **Administrar protección** contiene una lista de los componentes de Protección Antivirus.
- La sección **Tareas** contiene una lista de tareas locales que se ejecutan en el equipo.

Cada sección contiene elementos de control que puede utilizar para activar o desactivar el funcionamiento de un componente: vaya a la configuración del componente o tarea seleccionado y vea estadísticas de funcionamiento para el componente o tarea seleccionado.



Pestaña Protección y control de aplicaciones

Para abrir la pestaña *Protección y control de aplicaciones*, realice una de las siguientes acciones:

- En la [ventana principal de la aplicación](#), seleccione la pestaña **Protección y control**.
- Haga clic en el icono de la aplicación en el área de notificaciones de la barra de tareas de Microsoft Windows.
- Seleccione **Kaspersky Endpoint Security 10 para Windows** en el [menú contextual del icono de la aplicación](#).

Licencias de la aplicación

Esta sección ofrece información sobre los conceptos generales relacionados con las licencias de la aplicación.

Acerca del Contrato de licencia de usuario final

El *Contrato de licencia de usuario final* es un contrato vinculante entre usted y Kaspersky Lab AO en el que se estipulan los términos en los que puede utilizar la aplicación.

Le recomendamos que lea detenidamente los términos del Contrato de licencia antes de utilizar la aplicación.

Puede ver los términos del Contrato de licencia de las siguientes formas:

- Al instalar la aplicación de Kaspersky Endpoint Security en [modo interactivo](#).
- Mediante la lectura del archivo license.txt. Este documento se incluye en el [kit de distribución de la aplicación](#).

Al confirmar que está de acuerdo con el Contrato de licencia de usuario final mientras instala la aplicación, acepta los términos del Contrato de licencia de usuario final. Si no acepta los términos del Contrato de licencia de usuario final, debe cancelar la instalación.

Acerca de la licencia

Una *licencia* es un derecho de duración limitada para utilizar la aplicación garantizado en el Contrato de licencia de usuario final.

Una licencia válida le da derecho a los siguientes tipos de servicio:

- Uso de la aplicación de acuerdo con los términos del Contrato de licencia de usuario final
- Soporte técnico

La cobertura de los servicios y la duración del uso de la aplicación dependen del tipo de licencia que se haya utilizado para activar la aplicación.

Se proporcionan los siguientes tipos de licencia:

- *Licencia de evaluación*: Licencia gratuita destinada a probar la aplicación.
La licencia de evaluación suele durar poco tiempo. Cuando finaliza la licencia de evaluación, se desactivan todas las funciones de Kaspersky Endpoint Security. Para seguir utilizando la aplicación, debe comprar una licencia comercial.
Puede activar la aplicación con una licencia de prueba solo una vez.
- *Licencia comercial*: Licencia de pago que se facilita cuando compra Kaspersky Endpoint Security.
La funcionalidad de la aplicación que está disponible con licencia comercial depende del tipo de producto elegido. El producto seleccionado se indica en el [Certificado de licencia](#). Encontrará información sobre los productos disponibles en el [sitio web de Kaspersky](#).

Cuando la licencia comercial expira, las funciones clave de la aplicación se desactivan. Para seguir utilizando la aplicación, debe renovar la licencia comercial. Si no tiene pensado renovar la licencia, debe eliminar la aplicación del equipo.

Acerca del certificado de la licencia

Un *certificado de la licencia* es un documento transferido al usuario junto con un fichero llave o código de activación.

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

- Número de pedido
- Detalles del usuario a quien se concede la licencia
- Detalles de la aplicación que se puede activar con la licencia
- Límite de unidades autorizadas (por ejemplo, el número de dispositivos en los cuales la aplicación se puede utilizar con la licencia)
- Fecha de inicio del período de validez de la licencia
- Fecha de caducidad o período de validez de la licencia
- Tipo de licencia

Acerca de la suscripción

La *suscripción a Kaspersky Endpoint Security* es un pedido de compra de la aplicación con parámetros específicos (fecha de vencimiento de la suscripción, número de dispositivos protegidos). Puede solicitar una suscripción a Kaspersky Endpoint Security a través de su proveedor de servicios (por ejemplo, como su ISP). La suscripción puede renovarse manual o automáticamente, o bien puede cancelar su suscripción. Puede gestionar su suscripción en el [sitio web del proveedor de servicios](#).

Es posible aplicar límites a la suscripción (por ejemplo, un año) o cancelarlos (sin una fecha de vencimiento). Para mantener Kaspersky Endpoint Security en funcionamiento después del vencimiento del plazo de suscripción limitado, es necesario renovar la suscripción. La suscripción ilimitada se renueva automáticamente si los servicios del proveedor se han pagado por adelantado a tiempo.

En el caso de una suscripción limitada, a partir de su vencimiento se le ofrecerá un período de gracia para la renovación de la suscripción durante el cual la aplicación conservará su funcionalidad. El proveedor de servicios decide si conceder un período de gracia o no y, en caso de concederlo, determina la duración del período de gracia.

Para utilizar Kaspersky Endpoint Security mediante suscripción, debe aplicar el código de activación recibido del proveedor de servicios. Después de que se aplique el código de activación, se instala la clave activa. La clave activa define la licencia para usar la aplicación mediante suscripción. Puede instalarse una clave adicional solo con un código de activación y no con un archivo llave ni con una suscripción.

La funcionalidad de la aplicación disponible mediante suscripción puede corresponder a la funcionalidad de la aplicación para los tipos siguientes de licencias comerciales: Estándar, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Estos tipos de licencias están diseñados para proteger servidores de archivos, estaciones de trabajo y dispositivos móviles, y admiten el uso de componentes de control en estaciones de trabajo y dispositivos móviles.

Las opciones posibles de gestión de la suscripción pueden variar con cada proveedor de servicios. El proveedor de servicios puede no ofrecer un período de gracia para la renovación de la suscripción, durante el cual la aplicación conservará su funcionalidad.

Los códigos de activación adquiridos mediante suscripción pueden no utilizarse para activar versiones anteriores de Kaspersky Endpoint Security.

Acerca del código de activación

Un *código de activación* es una secuencia alfanumérica única de veinte dígitos y caracteres latinos que recibe al comprar una licencia comercial para Kaspersky Endpoint Security.

Para activar la aplicación con un código de activación, se requiere acceso a Internet con el fin de conectarse a servidores de activación de Kaspersky.

Cuando la aplicación se activa mediante un código de activación, se instala la clave activa. Puede instalarse una clave adicional solo con un código de activación y no con un archivo llave ni con una suscripción.

Si se extravía un código de activación después de activar la aplicación, se puede restaurar. Puede necesitar un código de activación, por ejemplo, para registrar una CompanyAccount de Kaspersky. Para restaurar un código de activación, se debe [poner en contacto con el Soporte Técnico de Kaspersky](#).

Acerca de la clave

Una *clave* es una secuencia alfanumérica única. Permite utilizar la aplicación en los términos indicados en el Contrato de licencia de usuario final (tipo de licencia, período de validez de la licencia, restricciones de la licencia).

Un certificado de la licencia no se proporciona para una clave instalada mediante suscripción.

Se puede agregar a la aplicación mediante un código de activación o un archivo llave.

Puede agregar, modificar o eliminar claves. Kaspersky puede bloquear la clave si se infringen los términos de Contrato de licencia de usuario final. Si la clave se ha incluido en la lista negra, deberá agregar otra clave distinta para continuar utilizando la aplicación.

Si se ha eliminado una clave de una licencia caducada, la funcionalidad de la aplicación no está disponible. No puede volver a agregar la clave después de que ha sido eliminada.

Existen dos tipos de claves: activa y adicional.

Una *clave activa* es aquella que utiliza actualmente la aplicación. Se puede agregar una licencia de clave de evaluación o comercial como clave activa. La aplicación solo podrá utilizar una única clave activa.

Una *clave adicional* es una clave que da derecho al usuario a utilizar la aplicación, pero que no se encuentra actualmente en uso. Cuando la clave activa vence, se activa automáticamente una clave adicional. Solo puede agregarse una clave adicional si la clave activa está disponible.

Una clave para una licencia de evaluación solo se puede agregar como una clave activa. No puede agregarse como la clave adicional. Una clave de licencia de evaluación no puede sustituir a la clave activa de una licencia comercial.

Si se incluye una clave en la lista negra, la funcionalidad de la aplicación definida por la [licencia bajo la que se ha activado la aplicación](#) sigue estando disponible durante ocho días. Kaspersky Security Network y las actualizaciones de la base de datos y los módulos de la aplicación están disponibles sin restricciones. La aplicación informa a ese usuario de que se ha incluido la clave en la lista negra. Transcurridos ocho días, la funcionalidad de la aplicación se limita al nivel disponible tras el vencimiento de la licencia (la aplicación funciona sin actualizaciones y el servicio Kaspersky Security Network no está disponible).

Acerca del archivo llave

Un *archivo clave* es un archivo con la extensión .key que recibe de Kaspersky después de adquirir Kaspersky Endpoint Security. El objetivo de este archivo llave es añadir una clave que active la aplicación.

No es necesario que se conecte con los servidores de activación de Kaspersky a fin de activar la aplicación con un archivo de clave.

Puede recuperar un archivo llave si se ha eliminado accidentalmente. Por ejemplo, es posible que necesite un archivo llave para registrarse en CompanyAccount de Kaspersky.

Para recuperar un archivo llave, realice uno de las siguientes acciones:

- Póngase en contacto con el vendedor de la licencia.
- Obtenga un archivo de clave en el [sitio web de Kaspersky](#) según su código de activación existente.

Cuando la aplicación se activa mediante un archivo clave, se agrega una clave activa. Puede añadirse una clave de licencia de reserva solo con un archivo clave y no con un código de activación.

Acerca de la provisión de datos

Al aceptar el Contrato de licencia de usuario final, acepta transferir automáticamente la información sobre el uso que le da al producto, así como el tipo, la versión y localización lingüística del programa instalado, el identificador exclusivo del instalador del programa y el tipo de instalación, y datos sobre claves activas y adicionales (incluidos el tipo de la licencia, el período de validez, la fecha de activación del programa y la de caducidad de la licencia, el número de la licencia, el estado actual de la licencia y la versión del protocolo de interacción del servidor de activación).

Si el programa se activa con un código de activación, a fin de recibir información estadística sobre la distribución y el uso de los productos del Titular de la Licencia, deberá aceptar proporcionar automáticamente la versión del programa utilizada (incluida la información sobre actualizaciones del programa instaladas, el identificador de instalación del programa e información sobre licencias), la versión del sistema operativo y los componentes identificadores del programa activos en el momento en que se proporciona la información.

La información recibida cuenta con protección de Kaspersky de acuerdo con la ley, los requisitos y las normativas aplicables de Kaspersky.

Kaspersky utiliza información que recibe de forma completamente anónima y solo en forma de datos estadísticos generales. Las estadísticas generales se generan automáticamente usando información recopilada originalmente y no contienen datos personales ni otra información confidencial. La información recopilada originalmente se destruye a medida que se acumula (una vez al año). Los datos estadísticos generales se almacenan indefinidamente.

Lea el Contrato de licencia de usuario final y visite el [sitio web de Kaspersky](#) para obtener más información sobre cómo recopilar, procesar, almacenar y destruir información del uso de la aplicación después de aceptar el Contrato de licencia de usuario final y la declaración de KSN. Los archivos license.txt y ksn.txt contienen el Contrato de licencia de usuario final y la declaración de KSN, y forman parte del [paquete de distribución](#) del programa.

Visualización de información de la licencia

Para ver información sobre la licencia:

1. Abra la [ventana principal de la aplicación](#).
2. Haga clic en el botón  /  situado en la parte inferior de la ventana principal de la aplicación.

Se abre la ventana **Licencia**. La información sobre la licencia se muestra en la sección situada en la parte superior de la ventana **Licencia**.

Compra de una licencia

Puede comprar una licencia después de instalar la aplicación. Cuando compra una licencia, recibe un código de activación o un archivo llave para [activar la aplicación](#).

Para adquirir una licencia:

1. Abra la [ventana principal de la aplicación](#).
2. Haga clic en el botón  /  situado en la parte inferior de la ventana principal de la aplicación.

Se abre la ventana **Licencia**.

3. En la ventana **Licencia**, siga uno de estos pasos:

- Si no se ha agregado ninguna clave o se ha agregado una clave de una licencia de evaluación, haga clic en el botón **Comprar la licencia**.
- Si se ha agregado la clave de una licencia comercial, haga clic en el botón **Renovar la licencia**.

Se abrirá una ventana con el sitio web de la tienda en línea de Kaspersky, en la que podrá comprar una licencia.

Renovación de licencias

Cuando su licencia esté a punto de caducar, podrá renovarla. Con ello, se asegurará de que su equipo permanece protegido cuando caduca la licencia actual y antes de que active la aplicación con una nueva licencia.

Para renovar una licencia:

1. [Obtenga](#) un código de activación de la aplicación o un archivo llave nuevos.
2. [Agregue una clave adicional](#) mediante el código de activación o el archivo llave que ha recibido.

De este modo, se agrega una [clave adicional](#). Esta se [activa](#) cuando caduca la licencia.

La actualización del estado de la clave de adicional a activa puede tardar en llevarse a cabo debido a la distribución de la carga entre los servidores de activación de Kaspersky.

Renovación de suscripciones

Cuando utiliza la aplicación mediante suscripción, Kaspersky Endpoint Security se pone en contacto automáticamente con el servidor de activación en intervalos específicos hasta que caduque su suscripción.

Si utiliza la aplicación mediante suscripción ilimitada, Kaspersky Endpoint Security comprueba automáticamente el servidor de activación en busca de claves renovadas en segundo plano. Si hay una clave disponible en el servidor de activación, la aplicación la agrega sustituyendo la clave anterior. De esta manera, la suscripción ilimitada de Kaspersky Endpoint Security se renueva sin la participación del usuario.



Si utiliza la aplicación mediante suscripción limitada, el día del vencimiento de la suscripción (o del período de gracia tras el vencimiento de la suscripción durante el que está disponible la renovación de la suscripción) Kaspersky Endpoint Security muestra una notificación y detiene el intento de renovación automática de la suscripción. En este caso, Kaspersky Endpoint Security se comporta de la misma forma que lo hace cuando [caduca una licencia comercial de la aplicación](#) (la aplicación funciona sin actualizaciones y el servicio Kaspersky Security Network no está disponible).

Puede renovar la suscripción [en el sitio web del proveedor de servicios](#).

Puede actualizar el estado de la suscripción manualmente en la ventana **Licencia**. Esto puede requerirse si se ha renovado la suscripción después del vencimiento del período de gracia y la aplicación no ha actualizado el estado de la suscripción automáticamente.

Consulta del sitio web del proveedor de servicios

Para visitar el sitio web del proveedor de servicios en la interfaz de la aplicación:

1. Abra la [ventana principal de la aplicación](#).
2. Haga clic en el botón  /  situado en la parte inferior de la ventana principal de la aplicación. Se abre la ventana **Licencia**.
3. En la ventana **Licencia**, haga clic en **Contacto con el proveedor de suscripciones**.

Acerca de los métodos de activación de la aplicación

La *Activación* es el proceso para activar una licencia que le permite utilizar una versión completa de la aplicación hasta que la licencia caduque. El proceso de activación de la aplicación implica agregar una clave.

Puede activar la aplicación de una de las siguientes formas:

- Al instalar la aplicación con la ayuda del [Asistente de configuración inicial](#). Puede agregar la clave activa de esta manera.
- Localmente en la interfaz de la aplicación, con el [Asistente de activación](#). Puede agregar la clave activa y la clave adicional de esta manera.
- De forma remota con la ayuda del paquete de software Kaspersky Security Center, mediante la [creación](#) y el posterior [inicio](#) de una tarea de adición de claves. Puede agregar la clave activa y la clave adicional de esta manera.
- De forma remota, mediante la distribución de claves y códigos de activación almacenados en el almacén de claves del servidor de administración de Kaspersky Security Center a los equipos cliente (consulte la *Guía de administrador de Kaspersky Security Center* para obtener más información). Puede agregar la clave activa y la clave adicional de esta manera.



En primer lugar, se distribuye el código de activación adquirido mediante suscripción.

- Mediante la [línea de comandos](#).

La activación de la aplicación con un código de activación puede llevar algún tiempo (durante la instalación remota o no interactiva), debido a la distribución de la carga a través de los servidores de activación de Kaspersky. Si necesita activar la aplicación inmediatamente, puede interrumpir la activación del proceso e iniciar la activación con el Asistente de activación.

Uso del asistente de activación para activar la aplicación

Para activar Kaspersky Endpoint Security mediante el asistente de activación:

1. Haga clic en el botón  /  situado en la parte inferior de la ventana principal de la aplicación.
Se abre la ventana **Licencia**.
2. En la ventana **Licencia**, haga clic en el botón **Activar la aplicación con una licencia nueva**.
Se inicia el Asistente de activación de la aplicación.
3. Siga las instrucciones del Asistente de activación.

Para obtener información más detallada sobre el procedimiento de activación de la aplicación, consulte la sección en el [Asistente de configuración inicial](#).

Activación de la aplicación desde la línea de comandos

Para activar la aplicación desde la línea de comandos,

escriba `avp.com license /add <código de activación o archivo llave> /password=
<contraseña>`.

Inicio y detención de la aplicación

En esta sección, se describe cómo puede configurar el inicio automático de la aplicación, iniciar o detener la aplicación de forma manual y detener o reanudar los componentes de protección y control.

Activación y desactivación de la ejecución automática de la aplicación

Por activación automática se entiende que Kaspersky Endpoint Security se inicia inmediatamente después de iniciarse el sistema operativo sin la intervención del usuario. Esta opción de ejecución de la aplicación está activada de forma predeterminada.

Después de su instalación, Kaspersky Endpoint Security se inicia automáticamente la primera vez. En veces sucesivas, la aplicación se inicia automáticamente después de iniciarse el sistema operativo.

La descarga de las bases de datos de Kaspersky Endpoint Security después de que se inicie el sistema operativo puede requerir hasta dos minutos según la capacidad del equipo. Durante este período, el nivel de protección del equipo se reduce. La descarga de bases de datos Anti-virus cuando Kaspersky Endpoint Security se inicia en un sistema operativo ya cargado no causa una reducción del nivel de protección del equipo.

Para activar o desactivar la ejecución automática de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).
2. Seleccione la sección **Protección Antivirus** situada a la izquierda.
La configuración de la protección antivirus se muestra en la parte derecha de la ventana.
3. Realice una de las siguientes acciones:
 - Si desea activar la ejecución automática de la aplicación, seleccione la casilla de verificación **Ejecutar Kaspersky Endpoint Security 10 para Windows al arrancar el equipo**.
 - Si desea desactivar la ejecución automática de la aplicación, desactive la casilla de verificación **Ejecutar Kaspersky Endpoint Security 10 para Windows al arrancar el equipo**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Inicio y detención manuales de la aplicación

Los expertos de Kaspersky no recomiendan detener manualmente Kaspersky Endpoint Security ya que, de hacerlo, el equipo y sus datos personales quedan expuestos a amenazas. Si fuera necesario, puede [suspender la protección del equipo](#) durante el tiempo que necesite, sin detener la aplicación.

Es necesario iniciar Kaspersky Endpoint Security manualmente si previamente ha desactivado el [inicio automático de la aplicación](#).

Para iniciar la aplicación manualmente:

En el menú **Inicio**, seleccione **Aplicaciones** → Κασπερσκυ Ενδοποινη Σχευριτη 10 παρα Ωινδοωσ.



Para detener la aplicación manualmente:

1. Haga clic con el botón derecho para acceder al menú contextual del icono de la aplicación que se encuentra en el área de notificaciones de la barra de tareas.
2. En el menú contextual, seleccione **Salir**.

Suspensión y reanudación de la protección y el control del equipo

La suspensión de la protección y el control del equipo implica la desactivación de todos los componentes de protección y control de Kaspersky Endpoint Security durante un tiempo.

El estado de la aplicación se muestra mediante el [icono de la aplicación en el área de notificaciones de la barra de tareas](#).

- El icono  indica que Protección y control del equipo se ha suspendido.
- El icono  indica que se ha desactivado la protección y el control del equipo.

La suspensión o reanudación de la protección y el control del equipo no afectan a las tareas de análisis o actualización.

Si se establece alguna conexión de red al mismo tiempo que suspende o reanuda la protección y el control del equipo, se muestra una notificación para indicar la finalización de dichas conexiones de red.

Para pausar la protección y el control del equipo:

1. Haga clic con el botón derecho para acceder al menú contextual del icono de la aplicación que se encuentra en el área de notificaciones de la barra de tareas.
2. En el menú contextual, seleccione **Pausar Protección y control**.
Se abre la ventana **Suspender la protección**.
3. Seleccione una de las siguientes opciones:
 - **Suspender durante el tiempo especificado:** la protección y el control del equipo se reanudan una vez que haya transcurrido la cantidad de tiempo especificada en la siguiente lista desplegable.
 - **Suspender hasta reiniciar:** La protección y el control del equipo se reanudan tras salir y volver a entrar en la aplicación o tras reiniciar el sistema operativo. Debe activarse el inicio automático de la aplicación para utilizar esta opción.
 - **Suspender:** La protección y el control del equipo se reanudarán cuando decida volver a activarlos.
4. Si seleccionó la opción **Suspender durante el tiempo especificado** durante el paso anterior, seleccione el intervalo correspondiente en la lista desplegable.

Para reanudar la protección y el control del equipo:

1. Haga clic con el botón derecho para acceder al menú contextual del icono de la aplicación que se encuentra en el área de notificaciones de la barra de tareas.

2. En el menú contextual, seleccione **Reanudar Protección y control**.

Puede reanudar la protección y el control del equipo en cualquier momento, independientemente de la opción de suspensión de protección y control del equipo que haya seleccionado anteriormente.

Protección del sistema de archivos del equipo. Antivirus de archivos

Esta sección contiene información sobre Antivirus de archivos, además de instrucciones sobre cómo configurar los parámetros del componente.

Acerca de Antivirus de archivos

El componente Antivirus de archivos protege el equipo frente a la infección del sistema de archivos. De forma predeterminada, el Antivirus de archivos se inicia con Kaspersky Endpoint Security, permanece activo todo el tiempo en la memoria del equipo y analiza todos los archivos que se abren, guardan o ejecutan en el equipo y en todas las unidades que se incorporan a él en busca de virus y otras amenazas.

Al detectar una amenaza en un archivo, Kaspersky Endpoint Security realiza las siguientes acciones:

1. Detecta el tipo de objeto encontrado en el archivo (como un *virus* o un *troyano*).
2. Etiqueta el archivo como *probablemente infectado* si el análisis no puede determinar si el archivo está infectado o no. Es posible que el archivo contenga una secuencia de código propia de un virus u otro software malintencionado (malware) o un código modificado de un virus conocido.
3. La aplicación muestra una [notificación](#) sobre el objeto malicioso que se detecta en el archivo (si se han configurado las notificaciones) y procesa el archivo aplicando la [acción](#) especificada en la configuración de Antivirus de archivos.

Activación y desactivación del Antivirus de archivos





De forma predeterminada, Antivirus de archivos está activado, ejecutándose en el modo recomendado por los expertos de Kaspersky. Si es necesario, puede desactivar el Antivirus de archivos.

Existen dos formas de activar o desactivar el componente:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

Para activar o desactivar Antivirus de archivos en la pestaña Protección y control de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Protección**.
Se abre la sección **Protección**.
4. Haga clic con el botón derecho para que aparezca el menú contextual de la línea con información sobre el componente Antivirus de archivos.
Se abre un menú para seleccionar acciones sobre los componentes.
5. Realice una de las siguientes acciones:

- Para activar Antivirus de archivos, seleccione **Iniciar** en el menú.
El icono de estado del componente , que se muestra a la izquierda en la línea **Antivirus de archivos**, cambia al icono .
- Para desactivar Antivirus de archivos, seleccione **Detener** en el menú.
El icono de estado del componente , que se muestra a la izquierda en la línea **Antivirus de archivos**, cambia al icono .

Para activar o desactivar Antivirus de archivos en la ventana de configuración de la aplicación:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus de archivos**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus de archivos.
3. Realice una de las siguientes acciones:
 - Si quiere activar el Antivirus de archivos, seleccione la casilla de verificación **Activar Antivirus de archivos**.
 - Si quiere desactivar el Antivirus de archivos, desactive la selección de la casilla de verificación **Activar Antivirus de archivos**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Suspensión automática del Antivirus de archivos

Puede configurar Antivirus de archivos para que se suspenda de forma automática a una hora concreta o cuando utilice determinados programas.

La suspensión del Antivirus de archivos es una medida de emergencia cuando entra en conflicto con algunos programas. Si se producen problemas durante el funcionamiento de un componente, le recomendamos que se ponga en contacto con el Soporte técnico de Kaspersky (<https://companyaccount.kaspersky.com>). Los especialistas de soporte le ayudarán a configurar Antivirus de archivos para que se ejecute de forma simultánea con otros programas de su equipo.

Para configurar la suspensión automática de Antivirus de archivos:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus de archivos**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus de archivos.
3. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
Se abre la ventana **Antivirus de archivos**.
4. En la ventana **Antivirus de archivos**, seleccione la pestaña **Avanzado**.
5. En la sección **Suspender tarea**:

- Para configurar la suspensión automática del Antivirus de archivos a una hora especificada, seleccione la casilla de verificación **Mediante planificación** y haga clic en el botón **Planificación**.

Se abre la ventana **Suspender tarea**.

- Para configurar la suspensión automática del Antivirus de archivos al iniciar aplicaciones concretas, seleccione la casilla de verificación **Al iniciar la aplicación** y haga clic en el botón **Seleccionar**.

Se abre la ventana **Aplicaciones**.

6. Realice una de las siguientes acciones:

- Si está configurando la suspensión automática de Antivirus de archivos a una hora concreta, en la ventana **Suspender tarea**, utilice los campos **Suspender la tarea a las** y **Reanudar la tarea a las** para especificar el período de tiempo (en formato HH:MM) durante el que se debe suspender Antivirus de archivos. Haga clic en **Aceptar**.
- Si está configurando la suspensión automática de Antivirus de archivos al iniciar determinadas aplicaciones, utilice los botones **Agregar**, **Editar** y **Eliminar** de la ventana **Aplicaciones** para crear una lista de aplicaciones durante cuyo funcionamiento se suspenderá Antivirus de archivos. Haga clic en **Aceptar**.

7. En la ventana **Antivirus de archivos**, haga clic en **Aceptar**.

8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Configuración del Antivirus de archivos

Puede hacer lo siguiente para configurar Antivirus de archivos:

- Modificar el nivel de seguridad.

Puede seleccionar uno de los niveles de seguridad predeterminados o ajustar manualmente la configuración del nivel de seguridad. Si cambia la configuración del nivel de seguridad, siempre puede volver a la configuración recomendada del nivel de seguridad.

- Cambiar la acción que lleva a cabo Antivirus de archivos al detectar un archivo infectado.

- Editar la cobertura de protección del Antivirus de archivos.

Puede ampliar o reducir la cobertura de protección agregando o quitando objetos para el análisis, o cambiando el tipo de los archivos que deben analizarse.

- Configurar el Analizador heurístico.

Antivirus de archivos utiliza una técnica denominada análisis de firmas. Durante el análisis de firmas, Antivirus de archivos equipara el objeto detectado con los registros de sus bases de datos de antivirus de la aplicación. Siguiendo las recomendaciones de los expertos de Kaspersky, el análisis de firmas está siempre activado.

Para aumentar la eficacia de la protección, puede usar el análisis heurístico. Durante el análisis heurístico, Antivirus de archivos analiza la actividad de los objetos en el sistema operativo. Análisis heurístico posibilita la detección de nuevos objetos maliciosos para los que no hay disponibles registros disponibles en las bases de datos de antivirus de la aplicación.

- Optimice el análisis.

Puede optimizar el análisis de archivos realizado por Antivirus de archivos, lo que reduce el tiempo de análisis y aumenta la velocidad de funcionamiento de Kaspersky Endpoint Security. Esto se puede conseguir si analiza solamente los archivos nuevos y los que se hayan modificado desde el último análisis. Este modo se aplica tanto a archivos simples como a compuestos.

También puede activar el uso de las tecnologías iChecker e iSwift, que optimizan la velocidad del análisis de archivos mediante la exclusión de archivos que no se han modificado desde el análisis más reciente.

- Configurar el análisis de archivos compuestos.
- Modificar el modo de análisis de archivos.

Cambiar el nivel de seguridad

Para proteger el sistema de archivos del equipo, Antivirus de archivos aplica varios grupos de parámetros de configuración. Estos grupos de parámetros de configuración se denominan *niveles de seguridad*. Existen tres niveles de seguridad predeterminados: **Máximo**, **Recomendado** y **Mínimo**. Se considera que la configuración del nivel de seguridad **Recomendado** es la configuración óptima recomendada por expertos de Kaspersky.

Para cambiar un nivel de seguridad:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus de archivos**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus de archivos.
3. En la sección **Nivel de seguridad**, lleve a cabo una de las siguientes acciones:
 - Si desea establecer uno de los niveles de seguridad predeterminados (**Máximo**, **Recomendado** o **Mínimo**), selecciónelo con el control deslizante.
 - Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración** y, en la ventana **Antivirus de archivos** que se abre, introduzca la configuración personalizada.
Después de configurar un nivel de seguridad personalizado, el nombre del nivel de seguridad de la sección **Nivel de seguridad** cambia a **Personalizado**.
 - Si desea cambiar el nivel de seguridad a **Recomendado**, haga clic en el botón **Predeterminado**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Modificación de la acción que Antivirus de archivos debe realizar en los archivos infectados

Para modificar la acción que Antivirus de archivos debe realizar en los archivos infectados:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus de archivos**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus de archivos.

3. En la sección **Acción al detectar una amenaza**, seleccione la opción requerida:

- **Seleccionar la acción automáticamente.**
- **Realizar acción: desinfectar Eliminar si falla la desinfección.**
- **Realizar acción: desinfectar.**

Incluso si se selecciona esta opción, Kaspersky Endpoint Security aplica la acción **Eliminar** a los archivos que forman parte de la aplicación Tienda Windows.

- **Realizar acción: quitar.**
- **Realizar acción: bloquear.**

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Edición de la cobertura de protección del Antivirus de archivos

La cobertura de protección hace referencia a los objetos que analiza el componente cuando está activado. Las coberturas de protección de los distintos componentes tienen distintas propiedades. La ubicación y el tipo de archivos que se van a analizar son propiedades de la cobertura de protección de Antivirus de archivos. De forma predeterminada, Antivirus de archivos analiza únicamente [archivos infectables](#) almacenados en discos duros, unidades de red o archivos extraíbles.

Para crear la Cobertura de protección:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus de archivos**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus de archivos.
3. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
Se abre la ventana **Antivirus de archivos**.
4. En la ventana **Antivirus de archivos**, seleccione la pestaña **General**.
5. En la sección **Tipos de archivos**, especifique el tipo de archivos que desea que Antivirus de archivos analice.
 - Si quiere analizar todos los archivos, seleccione **Todos los archivos**.
 - Si quiere analizar los archivos con los formatos más vulnerables a los virus, seleccione **Analizar archivos por formato**.
 - Si quiere analizar los archivos con las extensiones más vulnerables a los virus, seleccione **Analizar archivos por extensión**.

Al seleccionar el tipo de archivos que vayan a analizarse, recuerde la siguiente información:

- Existen algunos formatos de archivo (como .txt) para los que la probabilidad de intrusión de código malicioso y su posterior activación es bastante baja. De igual modo, otros formatos de archivos contienen o pueden contener código ejecutable (por ejemplo: .exe, .dll y .doc). Es bastante elevado el riesgo de penetración y activación de código malicioso en estos archivos.
- Un intruso puede enviar un virus u otro programa malicioso a su equipo en un archivo ejecutable al que se ha cambiado el nombre con la extensión .txt. Si selecciona el análisis de los archivos por extensión, en el análisis se omitirá este archivo. Si selecciona el análisis de archivos por formato, entonces, con independencia de la extensión, Antivirus de archivos analiza el encabezado del archivo. Este análisis puede revelar que el archivo tiene el formato .exe. Se analiza ese archivo minuciosamente en busca de virus y otro software malicioso (malware).

6. En la lista de **Cobertura de protección**, lleve a cabo una de las siguientes acciones:

- Haga clic en el botón **Agregar** si quiere agregar un objeto nuevo a la cobertura del análisis.
- Si quiere cambiar la ubicación de un objeto, seleccione el objeto de la cobertura del análisis y haga clic en el botón **Editar**.

Se abre la ventana **Seleccionar cobertura del análisis**.

- Si quiere eliminar un objeto de la lista de objetos que se van a analizar, selecciónelo y haga clic en el botón **Quitar**.

Se abre una ventana para que confirme la eliminación.

7. Realice una de las siguientes acciones:

- Si quiere agregar un nuevo objeto o cambiar la ubicación de un objeto de la lista de objetos que se van a analizar, seleccione el objeto en la ventana **Seleccionar cobertura de análisis** y haga clic en el botón **Agregar**.

Todos los objetos seleccionados en la ventana **Seleccionar cobertura del análisis** se muestran en la ventana **Antivirus de archivos**, en la lista **Cobertura de protección**.

Haga clic en **Aceptar**.

- Si quiere Eliminar un objeto, haga clic en el botón **Sí** de la ventana para confirmar la eliminación.

8. Si es necesario, repita los pasos 6 y 7 para agregar, mover o eliminar objetos de la lista de objetos que se van a analizar.

9. Para excluir un objeto de la lista de objetos que se van a analizar, quite la casilla de verificación que hay junto a los objetos de la lista **Cobertura de protección**. Sin embargo, el objeto permanece en la lista de objetos para escanear, aunque está excluido del análisis del Antivirus de archivos.

10. En la ventana **Antivirus de archivos**, haga clic en **Aceptar**.

11. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Uso del Analizador heurístico con Antivirus de archivos

Para configurar el uso del Analizador heurístico en el funcionamiento de Antivirus de archivos:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus de archivos**.

En la parte derecha de la ventana se muestra la configuración del componente Antivirus de archivos.

3. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.

Se abre la ventana **Antivirus de archivos**.

4. En la ventana **Antivirus de archivos**, seleccione la pestaña **Rendimiento**.

5. En la sección **Métodos de análisis**:

- Si quiere que Antivirus de archivos utilice el análisis heurístico, seleccione la casilla de verificación **Análisis heurístico** y utilice el control deslizante para definir el nivel de detalle del análisis heurístico: **Análisis superficial**, **Análisis medio** o **Análisis avanzado**.
- Si no quiere que Antivirus de archivos utilice el análisis heurístico, desactive la sección de la casilla de verificación **Análisis heurístico**.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Uso de tecnologías de análisis en el funcionamiento de Antivirus de archivos

Para configurar el uso de tecnologías de análisis en el funcionamiento de Antivirus de archivos:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus de archivos**.

En la parte derecha de la ventana se muestra la configuración del componente Antivirus de archivos.

3. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.

Se abre la ventana **Antivirus de archivos**.

4. En la ventana **Antivirus de archivos**, seleccione la pestaña **Avanzado**.

5. En la sección **Tecnologías de análisis**:

- Seleccione las casillas de verificación de los nombres de las tecnologías que quiera que use el Antivirus de archivos durante su funcionamiento.
- Desactive las casillas de verificación de los nombres de las tecnologías que no quiera que use el Antivirus de archivos durante su funcionamiento.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Optimización del análisis de archivos

Para optimizar el análisis de archivos:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus de archivos**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus de archivos.
3. Haga clic en el botón **Configuración**.
Se abre la ventana **Antivirus de archivos**.
4. En la ventana **Antivirus de archivos**, seleccione la pestaña **Rendimiento**.
5. En la sección **Optimización del análisis**, seleccione la casilla de verificación **Analizar solamente archivos nuevos y modificados**.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Análisis de archivos compuestos

Una técnica común para ocultar virus y otro tipo de malware consiste en implantarlos en archivos compuestos, como archivos comprimidos o bases de datos. Para detectar virus y otro tipo de software malicioso (malware) oculto de este modo, se debe descomprimir el archivo compuesto, lo que puede ralentizar el análisis. Puede limitar el conjunto de archivos compuestos que se deben analizar, lo que permite acelerar el análisis.

El método empleado para procesar un archivo compuesto infectado (desinfección o eliminación) depende del tipo de este.

Antivirus de archivos desinfecta archivos compuestos de formatos RAR, ARJ, ZIP, CAB y LHA, y elimina archivos del resto de los formatos (excepto bases de datos de correo).

Para configurar el análisis de archivos compuestos:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus de archivos**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus de archivos.
3. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
Se abre la ventana **Antivirus de archivos**.

4. En la ventana **Antivirus de archivos**, seleccione la pestaña **Rendimiento**.

5. En la sección **Análisis de archivos compuestos**, especifique los tipos de archivos compuestos que quiere analizar: archivos comprimidos, paquetes de instalación o archivos en formatos de Office.

6. Para analizar únicamente archivos compuestos nuevos y modificados, active la casilla de verificación **Analizar solamente archivos nuevos y modificados**.

Antivirus de archivos solo analizará archivos compuestos, nuevos y modificados, de todos los tipos.

7. Haga clic en el botón **Avanzado**.

Se abre la ventana **Archivos compuestos**.

8. En la sección **Análisis en segundo plano**, lleve a cabo una de las siguientes acciones:

- Para impedir que Antivirus de archivos desempaquete archivos compuestos en segundo plano, desactive la casilla de verificación **Extraer archivos compuestos en segundo plano**.
- Para permitir que Antivirus de archivos desempaquete archivos compuestos mientras analiza en segundo plano, seleccione la casilla de verificación **Extraer archivos compuestos en segundo plano** y especifique el valor requerido en el campo **Tamaño mínimo de archivo**.

9. En la sección **Límite de tamaño**, lleve a cabo una de las siguientes acciones:

- Si no quiere que Antivirus de archivos descomprima archivos compuestos de gran tamaño, active la casilla de verificación **No descomprimir archivos compuestos de gran tamaño** y especifique el valor requerido en el campo **Tamaño máximo de archivo**. Antivirus de archivos no desempaquetará los archivos compuestos con tamaños superiores al especificado.
- Si quiere que Antivirus de archivos descomprima archivos compuestos de gran tamaño, desactive la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**.

Un archivo se considera grande si su tamaño supera el valor del campo **Tamaño máximo de archivo**.

Antivirus de archivos analiza los archivos de gran tamaño extraídos de archivos comprimidos, con independencia de si se ha seleccionado o no la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**.

10. Haga clic en **Aceptar**.

11. En la ventana **Antivirus de archivos**, haga clic en **Aceptar**.

12. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Modificación del modo de análisis

Modo de análisis hace referencia a la condición que se debe dar para que Antivirus de archivos empiece a analizar archivos. De forma predeterminada, Kaspersky Endpoint Security analiza archivos en modo inteligente. En este modo de análisis de archivos, Antivirus de archivos decide si analizar o no archivos después de analizar las operaciones que lleva con el archivo el usuario, una aplicación en nombre del usuario (con la cuenta que se usó para iniciar la sesión o con una cuenta de usuario distinta) o el sistema operativo. Por ejemplo, Kaspersky Endpoint Security solo analiza un documento de Microsoft Office Word la primera vez que lo abre y cuando lo cierra. Las operaciones intermedias de escritura no provocan el análisis del archivo.

Para modificar el modo de análisis de archivos:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus de archivos**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus de archivos.
3. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
Se abre la ventana **Antivirus de archivos**.
4. En la ventana **Antivirus de archivos**, seleccione la pestaña **Avanzado**.
5. En la sección **Modo de análisis**, seleccione el modo requerido:
 - **Modo inteligente**.
 - **En acceso y modificación**.
 - **En acceso**.
 - **En ejecución**.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Protección del correo electrónico. Antivirus del correo

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security se instala en un equipo con [Microsoft Windows para servidores de archivos](#).

Esta sección contiene información sobre Antivirus del correo e instrucciones sobre cómo configurar los parámetros del componente.

Acerca de Antivirus del correo


El Antivirus del correo analiza los mensajes de correo electrónico entrantes y salientes en busca de virus y otras amenazas. Se inicia con Kaspersky Endpoint Security, permanece activo todo el tiempo en la memoria del equipo y analiza todos los mensajes que se enviaron o recibieron a través de los protocolos POP3, SMTP, IMAP, MAPI y NNTP. Si no se detectan amenazas en el mensaje, pasa a estar disponible para el usuario o es procesado.

Al detectar una amenaza en un mensaje de correo electrónico, Antivirus del correo realiza lo siguiente:

1. Detecta el tipo de objeto encontrado en el mensaje de correo electrónico (como un *troyano*).
2. Se asigna uno de los estados siguientes a un mensaje de correo electrónico:
 - *Probablemente infectado*. Este estado se asigna si el análisis no puede determinar si el mensaje de correo electrónico está infectado definitivamente. Es posible que el mensaje contenga una sección de código que es típica de virus y otro malware, o bien código modificado de un virus conocido.
 - *Infectado*. Este estado se asigna a un objeto si el análisis de un mensaje de correo electrónico encuentra una sección de código de un virus conocido incluido en las bases de datos antivirus de Kaspersky Endpoint Security.
 - *No se encuentra*. Este estado se asigna a un objeto si el análisis de un mensaje de correo electrónico no detecta virus ni otras amenazas.

Por consiguiente, la aplicación bloquea el mensaje de correo electrónico, muestra una [notificación](#) sobre el objeto que ha detectado (si esta opción se ha especificado en la configuración de las notificaciones) y lleva a cabo la acción especificada en la configuración de Antivirus del correo.

Este componente interactúa con los clientes de correo instalados en el equipo. Hay una extensión integrable, disponible para el cliente del correo Microsoft Office Outlook®, que le permite poner a punto la configuración de análisis de mensajes. La extensión Antivirus del correo se incrusta en el programa de correo Microsoft Office Outlook durante la instalación de Kaspersky Endpoint Security.

El funcionamiento de Antivirus del correo se indica por medio del icono de la aplicación que se muestra en el área de notificaciones de la barra de tareas. Cuando Antivirus del correo analiza un mensaje de correo electrónico, el icono de la aplicación cambia a .

Activación y desactivación de Antivirus del correo

De forma predeterminada, Antivirus del correo está activado, y se ejecuta en el modo recomendado por los expertos de Kaspersky. Si es necesario, puede desactivar el Antivirus del correo.





Existen dos formas de activar o desactivar el componente:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

Para activar o desactivar Antivirus del correo en la pestaña Protección y control de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Protección**.
Se abre la sección **Protección**.
4. Haga clic con el botón derecho para que aparezca el menú contextual de la línea con información sobre el componente Antivirus del correo.
Se abre un menú para seleccionar acciones sobre los componentes.

5. Realice una de las siguientes acciones:

- Para activar Antivirus del correo, seleccione **Iniciar** en el menú.
El icono de estado del componente , que se muestra a la izquierda en la línea **Antivirus del correo**, cambia al icono .
- Para desactivar Antivirus del correo, seleccione **Detener** en el menú.
El icono de estado del componente , que se muestra a la izquierda en la línea **Antivirus del correo**, cambia al icono .

Para activar o desactivar Antivirus del correo en la ventana de configuración de la aplicación:

1. Abra la ventana de configuración de la aplicación.
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus del correo**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus del correo.
3. Realice una de las siguientes acciones:
 - Si quiere activar el Antivirus del correo, seleccione la casilla de verificación **Activar Antivirus del correo**.
 - Si quiere desactivar el Antivirus del correo, desactive la casilla de verificación **Activar Antivirus del correo**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Configuración de Antivirus del correo

Puede hacer lo siguiente para configurar Antivirus del correo:

- Cambie el nivel de seguridad del correo.

Puede seleccionar uno de los niveles de seguridad del correo electrónico preinstalados o configurar un nivel de seguridad del correo electrónico personalizado.

Si ha cambiado la configuración del nivel de seguridad del correo, siempre puede volver a la configuración recomendada del nivel de seguridad del correo.

- Cambie la acción que realiza Kaspersky Endpoint Security ante los mensajes infectados.
- Editar la cobertura de protección del Antivirus del correo.
- Configurar el análisis de archivos compuestos adjuntos a mensajes de correo electrónico:
Puede activar o desactivar el análisis de adjuntos del mensaje, limitar el tamaño máximo de los adjuntos de los mensajes para su análisis y limitar la duración máxima del análisis del adjunto del mensaje.
- Configure el filtrado por tipo de adjuntos de mensajes de correo electrónico.
El filtrado de adjuntos de mensajes por tipo permite renombrar o eliminar automáticamente los archivos de los tipos especificados.
- Configurar el Analizador heurístico.
Para aumentar la eficacia de la protección, puede usar el [análisis heurístico](#). Durante el análisis heurístico, Kaspersky Endpoint Security analiza la actividad de las aplicaciones en el sistema operativo. El análisis heurístico puede detectar amenazas en mensajes para las que no existen registros actualmente en las bases de datos de Kaspersky Endpoint Security.
- Configurar el análisis del correo en Microsoft Office Outlook.
Hay una extensión que se puede integrar, disponible para el cliente del correo Microsoft Office Outlook, que permite configurar adecuadamente los ajustes de análisis del correo electrónico.
Cuando trabaja con otros clientes de correo electrónico, incluidos Microsoft Outlook Express®, Windows Mail y Mozilla™ Thunderbird™, el componente Antivirus del correo analiza el tráfico de los protocolos de correo electrónico SMTP, POP3, IMAP y NNTP.

Al trabajar con el cliente de correo electrónico Mozilla Thunderbird, si se utilizan filtros para mover mensajes fuera de la carpeta **Bandeja de entrada**, Antivirus del correo no analiza mensajes de correo electrónico transmitidos mediante el protocolo IMAP en busca de virus y otras amenazas.

Modificación del nivel de seguridad del correo

Antivirus del correo aplica varios grupos de parámetros para proteger el correo. Estos grupos de parámetros se denominan *niveles de seguridad del correo electrónico*. Existen tres niveles de seguridad de correo electrónico: **Máximo**, **Recomendado** y **Mínimo**. El nivel de seguridad de archivos **Recomendado** se considera la configuración óptima y es el que recomienda Kaspersky.

Para modificar el nivel de seguridad en el correo electrónico:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus del correo**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus del correo.
3. En la sección **Nivel de seguridad**, lleve a cabo una de las siguientes acciones:

- Si quiere instalar uno de los tres niveles de seguridad de correo electrónico preinstalados (**Máximo**, **Recomendado** o **Mínimo**), utilice el control deslizante para seleccionar uno.
 - Si quiere configurar un nivel de seguridad de correo electrónico personalizado, haga clic en el botón **Configuración** y especifique la configuración en la ventana **Antivirus del correo**.
Después de configurar un nivel de seguridad del correo electrónico personalizado, el nombre del nivel de seguridad de la sección **Nivel de seguridad** cambia a **Personalizado**.
 - Si quiere cambiar el nivel de seguridad del correo electrónico a **Recomendado**, haga clic en el botón **Predeterminado**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Modificación de las acciones que se van a realizar en mensajes de correo electrónico infectados

Para cambiar la acción que se debe realizar con los mensajes de correo electrónico infectados:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus del correo**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus del correo.
3. En la sección **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security cuando se detecta un mensaje infectado.
 - **Seleccionar la acción automáticamente.**
 - **Realizar acción: desinfectar Eliminar si falla la desinfección.**
 - **Realizar acción: desinfectar.**
 - **Realizar acción: quitar.**
 - **Realizar acción: bloquear.**
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Edición de la Cobertura de protección del Antivirus del correo

La cobertura de protección hace referencia a los objetos que son analizados por el componente cuando este está activo. Las coberturas de protección de los distintos componentes tienen distintas propiedades. Las propiedades de la cobertura de protección de Antivirus del correo incluyen los ajustes para integrar Antivirus del correo en clientes de correo electrónico, así como el tipo de mensajes de correo electrónico y los protocolos de correo electrónico cuyo tráfico analiza Antivirus del correo. De forma predeterminada, Kaspersky Endpoint Security analiza los mensajes de correo entrante y saliente, así como el tráfico, a través de los protocolos POP3, SMTP, NNTP e IMAP, y se integra en los clientes de correo electrónico Microsoft Office Outlook.

Para crear la cobertura de protección del Antivirus del correo:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus del correo**.

En la parte derecha de la ventana se muestra la configuración del componente Antivirus del correo.

3. Haga clic en el botón **Configuración**.

Se abre la ventana **Antivirus del correo**.

4. Seleccione la pestaña **General**.

5. En la sección de **Cobertura de protección**, lleve a cabo una de las siguientes acciones:

- Si quiere que Antivirus del correo analice todos los mensajes entrantes y salientes del equipo, seleccione la opción **Mensajes entrantes y salientes**.
- Si quiere que Antivirus del correo solo analice los mensajes entrantes del equipo, seleccione la opción **Solo mensajes entrantes**.

Si elige analizar solo los mensajes entrantes, recomendamos que lleve a cabo un único análisis de todos los mensajes salientes, ya que existe la posibilidad de que su equipo tenga gusanos del correo electrónico que se distribuyan por correo. Esto ayuda a evitar problemas provocados por un envío masivo e incontrolado por correo electrónico de mensajes infectados desde su equipo.

6. En la sección **Conectividad**, haga lo siguiente:

- Si quiere que Antivirus del correo analice los mensajes transmitidos mediante los protocolos POP3, SMTP, NNTP e IMAP antes de que lleguen a su equipo, active la casilla de verificación **Tráfico POP3/SMTP/NNTP/IMAP**.

Si no quiere que Antivirus del correo analice los mensajes transmitidos mediante los protocolos POP3, SMTP, NNTP e IMAP antes de que lleguen a su equipo, desactive la casilla de verificación **Tráfico POP3/SMTP/NNTP/IMAP**. En este caso, los mensajes son analizados por la extensión Antivirus del correo integrada en el cliente del correo Microsoft Office Outlook después de que se reciban en el equipo del usuario si se selecciona la casilla de verificación **Avanzado: extensión para Microsoft Office Outlook**.

Si utiliza un cliente de correo electrónico distinto de Microsoft Office Outlook, los mensajes de correo electrónico transmitidos mediante los protocolos POP3, SMTP, NNTP e IMAP no se analizan por Antivirus del correo si se desactiva la casilla de verificación **Tráfico POP3/SMTP/NNTP/IMAP**.

- Si quiere permitir el acceso a la configuración de Antivirus del correo desde Microsoft Office Outlook y activar el análisis de mensajes transmitidos mediante los protocolos POP3, SMTP, NNTP, IMAP y MAPI después de que lleguen al equipo mediante una extensión incrustada en Microsoft Office Outlook, seleccione la casilla de verificación **Avanzado: extensión para Microsoft Office Outlook**.

Si quiere bloquear el acceso a la configuración de Antivirus del correo desde Microsoft Office Outlook y desactivar el análisis de mensajes transmitidos mediante los protocolos POP3, SMTP, NNTP, IMAP y MAPI después de que lleguen al equipo mediante una extensión integrada en Microsoft Office Outlook, desactive la casilla de verificación **Avanzado: extensión para Microsoft Office Outlook**.

La extensión Antivirus del correo se incrusta en el programa de correo Microsoft Office Outlook durante la instalación de Kaspersky Endpoint Security.

7. Haga clic en **Aceptar**.

8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Analizar archivos compuestos adjuntos a mensajes de correo electrónico

Para configurar el análisis de archivos compuestos adjuntos a mensajes de correo electrónico:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus del correo**.

En la parte derecha de la ventana se muestra la configuración del componente Antivirus del correo.

3. Haga clic en el botón **Configuración**.

Se abre la ventana **Antivirus del correo**.

4. Seleccione la pestaña **General**.

5. Realice lo siguiente en la sección **Análisis de archivos compuestos**:

- Si quiere que Antivirus del correo omita los archivos comprimidos adjuntos a mensajes, desactive la casilla de verificación **Analizar archivos comprimidos adjuntos**.
- Si quiere que Antivirus del correo omita adjuntos del correo electrónico que tengan un tamaño superior a N megabytes, seleccione la casilla de verificación **No analizar archivos comprimidos mayores de N MB**. Si selecciona esta casilla de verificación, especifique el tamaño máximo de los archivos comprimidos en el campo situado frente al nombre de la casilla de verificación.
- Si quiere que Antivirus del correo ignore el análisis de los adjuntos al correo electrónico que duren más de N segundos, desactive la casilla de verificación **No analizar archivos durante más de N seg**.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Filtrar adjuntos de mensajes de correo electrónico

Los programas maliciosos se pueden distribuir en forma de adjuntos del correo electrónico. Puede configurar el filtrado según el tipo de adjuntos del mensaje de modo que los archivos de los tipos especificados se renombran o eliminan automáticamente. Al volver a asignar un nombre a un tipo determinado de adjunto, Kaspersky Endpoint Security es capaz de proteger su equipo contra la ejecución automática de un programa malicioso.

Para configurar el filtrado de archivos adjuntos:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus del correo**.


En la parte derecha de la ventana se muestra la configuración del componente Antivirus del correo.

3. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.

Se abre la ventana **Antivirus del correo**.

4. En la ventana **Antivirus del correo**, seleccione la pestaña **Filtrado de adjuntos**.

5. Realice una de las siguientes acciones:

- Si no quiere que Antivirus del correo filtre adjuntos del correo electrónico, seleccione la opción **Desactivar el filtrado**.
- Si quiere que Antivirus del correo cambie el nombre de los adjuntos del correo electrónico de los [tipos especificados](#) , seleccione la opción **Renombrar los tipos de adjuntos especificados**.

Recuerde que el formato real de un archivo puede no corresponder al formato indicado por su extensión.

Si activa el filtrado de objetos adjuntos a mensajes de correo electrónico, Antivirus del correo puede eliminar o cambiar el nombre de archivos con las siguientes extensiones:

com: archivo ejecutable de una aplicación no superior a 64 KB

exe: archivo ejecutable o archivo comprimido autoextraíble

sys: archivo del sistema de Microsoft Windows

prg: texto de programas como dBase™, Clipper, Microsoft Visual FoxPro® o WAVmaker

bin: archivo binario

bat: archivo de lotes

cmd: archivo de comandos para Microsoft Windows NT (similar a un archivo bat para DOS), OS/2

dpl: biblioteca comprimida de Borland Delphi

dll: biblioteca de enlaces dinámicos

scr: pantalla de presentación en Microsoft Windows

cpl: módulo del panel de control de Microsoft Windows

ocx: objeto Microsoft OLE (Object Linking and Embedding)

tsp: programa ejecutable en modo de tiempo fraccionado

drv: controlador de dispositivo

vxd: controlador de dispositivo virtual de Microsoft Windows

pif: archivo de información de programa

lnk: archivo de acceso directo de Microsoft Windows

reg: archivo de claves para el Registro del sistema de Microsoft Windows

ini: archivo de configuración que contiene datos de instalación para Microsoft Windows, Windows NT y ciertas aplicaciones

cla: clase Java

vbs: script Visual Basic®

vbe: extensión de vídeo del BIOS

js, jse: texto de origen JavaScript

htm: documento hipertexto

htt: encabezado de hipertexto de Microsoft Windows

hta: programa hipertexto para Microsoft Internet Explorer®

asp: secuencia de comandos Active Server Pages

chm: archivo HTML compilado

pht: archivo HTML con scripts PHP integrados

php: script PHP integrado en archivos HTML

wsh: archivo de configuración de Microsoft Windows Script Host

wsf: script Microsoft Windows

the: papel tapiz del escritorio de Microsoft Windows 95

hlp: archivo de Ayuda de Microsoft Windows

eml: mensaje de correo de Microsoft Office Outlook Express

nws: mensaje de noticias de Microsoft Outlook Express

msg: mensaje de correo de Microsoft Mail

plg: mensaje de correo

mbx: extensión para mensajes de correo guardados de Microsoft Office Outlook

doc*: documentos de Microsoft Office Word, como doc (Microsoft Office Word), docx (Microsoft Office Word 2007 con compatibilidad con XML) y docm (Microsoft Office Word 2007 con compatibilidad para macros)

dot*: plantilla de documento de Microsoft Office Word, como: dot para plantillas de documento de Microsoft Office Word; dotx para plantillas de documento Microsoft Office Word 2007, y dotm para plantilla de documento Microsoft Office Word 2007 con soporte para macros

fpm: programa de bases de datos, archivo de inicio para Microsoft Visual FoxPro

rtf: documento en formato de texto enriquecido (Rich Text Format)

shs: fragmento de identificador de objeto de recorte de Shell de Windows

dwg: base de datos de dibujos de AutoCAD®

msi: paquete de instalación de Microsoft Windows Installer

otm: proyecto VBA para Microsoft Office Outlook

pdf: documento Adobe Acrobat

swf: objeto empaquetado Shockwave® Flash

jpg, jpeg: formato gráfico para imágenes comprimidas

emf: formato de metadatos ampliado Próxima generación de metadatos del SO Microsoft Windows. Las versiones de 16 bits de Microsoft Windows no admiten archivos EMF.

ico: archivo de icono

ov?: Archivos ejecutables de Microsoft Office Word

xl*: documentos de Microsoft Office Excel y archivos como: xla, la extensión para Microsoft Office Excel; xlc para diagramas; xlt para plantillas de documentos;.xlsx para libros de trabajo de Microsoft Office Excel 2007; xltm para libros de trabajo de Microsoft Office Excel 2007 con compatibilidad para macros; xlsb para libros de trabajo de Microsoft Office Excel 2007 en formato binario (no XML); xltx para plantillas de Microsoft Office Excel 2007; xlsx para plantillas de Microsoft Office Excel 2007 con compatibilidad para macros, y xlam para complementos de Microsoft Office Excel 2007 con compatibilidad para macros

pp*: documentos y archivos de Microsoft Office PowerPoint®, como: pps para diapositivas de Microsoft Office PowerPoint; ppt para presentaciones; pptx para presentaciones de Microsoft Office PowerPoint 2007; pptm para presentaciones de Microsoft Office PowerPoint 2007 con compatibilidad para macros; potx para plantillas de presentación de Microsoft Office PowerPoint 2007; potm para plantillas de presentación de Microsoft Office PowerPoint 2007 con compatibilidad para macros; ppsx para presentaciones de diapositivas de Microsoft Office PowerPoint 2007; ppsm para presentaciones de diapositivas de Microsoft Office PowerPoint 2007 con compatibilidad para macros, y ppam para complementos de Microsoft Office PowerPoint 2007 con compatibilidad para macros

md*: documentos y archivos de Microsoft Office Access® como mda para grupos de trabajo de Microsoft Office Access y mdb para bases de datos

sldx: diapositivas Microsoft PowerPoint 2007

sldm: diapositivas Microsoft PowerPoint 2007 con soporte para macros

thmx: tema Microsoft Office 2007

- Si quiere que Antivirus del correo elimine los adjuntos de los mensajes de los tipos especificados, seleccione la opción **Quitar los tipos de adjuntos especificados**.
6. Si seleccionó la opción **Renombrar los tipos de adjuntos especificados** o **Eliminar los tipos de adjuntos especificados** durante el paso anterior, seleccione las casillas de verificación situadas junto a los tipos de archivos pertinentes.
- Puede cambiar la lista de tipos de archivo con los botones **Agregar**, **Modificar** y **Eliminar**.
7. Haga clic en **Aceptar**.
8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Análisis de correos electrónicos en Microsoft Office Outlook

Durante la instalación de Kaspersky Endpoint Security, la extensión Antivirus del correo se incrusta en Microsoft Office Outlook (en adelante, también denominado Outlook). Le permite abrir la configuración del Antivirus del correo desde Outlook y especificar en qué momento desea que se analicen los mensajes de correo en busca de virus y otras amenazas. La extensión Antivirus del correo para Outlook puede analizar los mensajes entrantes y salientes que se transmiten mediante los protocolos POP3, SMTP, NNTP, IMAP y MAPI.

Los parámetros de Antivirus del correo pueden configurarse directamente desde Outlook si se selecciona la casilla de verificación **Avanzado: extensión para Microsoft Office Outlook** en la interfaz de Kaspersky Endpoint Security.

En Outlook, los mensajes entrantes de correo electrónico se analizan primero mediante Antivirus del correo (al seleccionar la casilla **Tráfico POP3 / SMTP / NNTP / IMAP** en la interfaz de Kaspersky Endpoint Security) y, a continuación, mediante la extensión Antivirus del correo incrustada en Outlook. Si Antivirus del correo detecta un objeto malicioso en un mensaje, le alerta sobre ello.

La opción que elija en la ventana de notificación determina qué componente elimina la amenaza en el mensaje de correo electrónico: Antivirus del correo o la extensión Antivirus del correo para Outlook.

- Si selecciona **Desinfectar** o **Eliminar** en la ventana de notificación, el Antivirus del correo se encarga de eliminar esta amenaza.
- Si selecciona **Omitir** en la ventana de notificación del usuario, la extensión Antivirus del correo para Outlook elimina la amenaza.

Los mensajes salientes son analizados primero por la extensión Antivirus del correo para Outlook y, a continuación, los analiza Antivirus del correo.

Configurar el análisis del correo en Outlook

Para configurar el análisis del correo en Outlook 2007:

1. Abra la ventana principal de Outlook 2007.
2. Seleccione **Servicio** **Configuración** en la barra de menú.
Se abre la ventana **Opciones**.
3. En la ventana **Opciones**, seleccione la pestaña **Protección del correo**.

Para configurar el análisis del correo en Outlook 2010/2013:

1. Abra la ventana principal de Outlook.
Seleccione la pestaña **Archivo** en la esquina superior izquierda.
2. Haga clic en el botón **Opciones**.
Se abre la ventana **Opciones de Outlook**.
3. Seleccione la sección **Complementos**.

La configuración de los complementos integrados en Outlook se muestra en la parte derecha de la ventana.

4. Haga clic en el botón **Opciones de complementos**.

Configurar el análisis del correo utilizando Kaspersky Security Center

Si el correo se maneja mediante la extensión Antivirus del correo para Outlook, se recomienda utilizar el modo caché de Exchange. Para obtener información más detallada sobre el modo de almacenamiento en caché de Exchange y las recomendaciones de uso, consulte la base de conocimientos de Microsoft: <https://technet.microsoft.com/es-es/library/cc179175.aspx>.

Para configurar el modo de funcionamiento de la extensión Antivirus del correo para Outlook con Kaspersky Security Center:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea configurar el análisis del correo.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Protección antivirus**, seleccione el apartado **Antivirus del correo**.
7. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
Se abre la ventana **Antivirus del correo**.
8. En la sección **Conectividad**, haga clic en el botón **Configuración**.
Se abre la ventana **Protección del correo**.
9. En la ventana **Protección del correo**:
 - Seleccione la casilla de verificación **Análisis al recibir** si desea que la extensión de Antivirus del correo para Outlook analice los mensajes entrantes cuando llegan al buzón de correo.
 - Seleccione la casilla de verificación **Análisis al leer** si desea que la extensión de Antivirus del correo para Outlook analice los mensajes entrantes cuando el usuario los abra.
 - Seleccione la casilla de verificación **Análisis al enviar** si desea que la extensión de Antivirus del correo para Outlook analice los mensajes salientes a medida que se envían.
10. En la ventana **Protección del correo**, haga clic en **Aceptar**.

11. En la ventana **Antivirus del correo**, haga clic en **Aceptar**.

12. Aplique la directiva.

Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

Protección del equipo en Internet. Antivirus Internet

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security se instala en un equipo con [Microsoft Windows para servidores de archivos](#).

Esta sección contiene información sobre Antivirus Internet e instrucciones sobre cómo configurar los parámetros del componente.

Acerca de Antivirus Internet

Cada vez que se conecta a Internet, expone la información que tiene almacenada en su equipo a virus y otro software malicioso (malware). Pueden infiltrarse en el equipo mientras el usuario descarga software gratuito o navega por sitios web cuya seguridad está en peligro por culpa de delincuentes. Los gusanos que hay en la red pueden encontrar la manera de acceder a su equipo en cuanto se inicie una conexión a Internet, incluso antes de que abra una página web o descargue un archivo.

Antivirus Internet protege los datos entrantes y salientes que se envían y reciben a través del equipo mediante protocolos FTP y HTTP. También, comprueba las direcciones URL por medio de la lista de direcciones web maliciosas o fraudulentas.

Antivirus Internet intercepta y analiza virus y otras amenazas en cada página web o archivo a los que el usuario o una aplicación acceden mediante el protocolo FTP o HTTP. Esto es lo que sucede después:

- Si no se encuentra código malicioso en la página o en el archivo, el usuario obtiene un acceso inmediato a él.
- Si un usuario accede a una página web o a un archivo que contenga código malicioso, la aplicación realiza la acción que se especifica en la configuración de Antivirus Internet.

Activación y desactivación del Antivirus Internet

De forma predeterminada, Antivirus Internet está activado, ejecutándose en el modo recomendado por los expertos de Kaspersky. Si es necesario, puede desactivar el Antivirus Internet.

Existen dos formas de activar o desactivar el componente:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

Para activar o desactivar Antivirus Internet en la pestaña Protección y control de la ventana principal de la aplicación:



1. Abra la ventana principal de la aplicación.
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Protección**.
Se abre la sección **Protección**.

4. Haga clic con el botón derecho para que aparezca el menú contextual de la línea con información sobre el componente Antivirus Internet.



Se abre un menú para seleccionar acciones sobre los componentes.

5. Realice una de las siguientes acciones:

- Para activar Antivirus Internet, seleccione **Iniciar** en el menú.

El icono de estado del componente , que se muestra a la izquierda en la línea **Antivirus Internet**, cambia al icono .

- Para desactivar Antivirus Internet, seleccione **Detener** en el menú.

El icono de estado del componente , que se muestra a la izquierda en la línea **Antivirus Internet**, cambia al icono .

Para activar o desactivar Antivirus Internet en la ventana de configuración de la aplicación:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus Internet**.

En la parte derecha de la ventana se muestra la configuración del componente Antivirus Internet.

3. Realice una de las siguientes acciones:

- Si quiere activar el Antivirus Internet, seleccione la casilla de verificación **Activar Antivirus Internet**.
- Si quiere desactivar el Antivirus Internet, desactive la casilla de verificación **Activar Antivirus Internet**.

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Configuración de Antivirus Internet

Puede hacer lo siguiente para configurar Antivirus Internet:

- Cambiar el nivel de seguridad de tráfico web.

Puede seleccionar uno de los niveles de seguridad preinstalados para el tráfico web que se recibe o se transmite a través de los protocolos HTTP y FTP, o configurar un nivel de seguridad del tráfico web personalizado.

Si cambia la configuración del nivel de seguridad del tráfico web, siempre podrá volver a la configuración del nivel de seguridad recomendada del tráfico web.

- Cambiar la acción que realiza Kaspersky Endpoint Security ante objetos de tráfico web maliciosos.

Si el análisis de un objeto HTTP muestra que contiene código malicioso, la respuesta de Antivirus Internet depende de la acción especificada.

- Configurar el análisis de direcciones URL con bases de datos de direcciones web maliciosas y fraudulentas por parte de Antivirus Internet.
- Configurar el uso del análisis heurístico cuando se analiza el tráfico web en busca de virus y otros programas maliciosos.

Para aumentar la eficacia de la protección, puede usar el análisis heurístico. Durante el análisis heurístico, Kaspersky Endpoint Security analiza la actividad de las aplicaciones en el sistema operativo. El análisis heurístico puede detectar amenazas para las que no existen registros actualmente en las bases de datos de Kaspersky Endpoint Security.

- Configurar el uso del análisis heurístico cuando se analizan páginas web en busca de enlaces fraudulentos.
- Optimice el análisis de Antivirus Internet de tráfico web enviado y recibido a través de los protocolos HTTP y FTP.
- Crear una lista de direcciones URL de confianza.

Puede crear una lista de direcciones URL en cuyo contenido confía. Antivirus Internet no analiza la información de direcciones URL de confianza en busca de virus u otras amenazas. Esta opción es útil, por ejemplo, cuando el componente Antivirus Internet interfiere en la descarga de un archivo de un sitio web conocido.

Una dirección URL puede ser la dirección de una página web concreta o de la dirección de un sitio web.

Modificación del nivel de seguridad del tráfico web

Para proteger los datos recibidos y transmitidos a través de los protocolos HTTP y FTP, Antivirus Internet aplica distintos grupos de parámetros de configuración. Estos grupos de parámetros se denominan *niveles de seguridad del tráfico web*. Existen tres niveles de seguridad del tráfico web: **Máxima**, **Recomendada** y **Mínima**. El nivel de seguridad del tráfico web **Recomendado** se considera la configuración óptima y es el que recomienda Kaspersky.

Para modificar el nivel de seguridad del tráfico web:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus Internet**.

En la parte derecha de la ventana se muestra la configuración del componente Antivirus Internet.

3. En la sección **Nivel de seguridad**, lleve a cabo una de las siguientes acciones:

- Si quiere instalar uno de los tres niveles de seguridad del tráfico web preinstalados (**Máximo**, **Recomendado** o **Mínimo**), utilice el control deslizante para seleccionar uno.
- Si quiere configurar un nivel de seguridad del tráfico web personalizado, haga clic en el botón **Configuración** y especifique la configuración en la ventana **Antivirus Internet**.
Si ha configurado un nivel de seguridad del tráfico web personalizado, el nombre del nivel de seguridad en la sección **Nivel de seguridad** cambia a **Personalizado**.
- Si quiere cambiar el nivel de seguridad del tráfico web a **Recomendado**, haga clic en el botón **Predeterminado**.

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Modificación de las acciones que se van a realizar en objetos maliciosos del tráfico web

Para cambiar la acción que se va a realizar en objetos maliciosos del tráfico web:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus Internet**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus Internet.
3. En la sección **Acción al detectar una amenaza**, seleccione la acción que lleva a cabo Kaspersky Endpoint Security en objetos maliciosos del tráfico web:
 - **Seleccionar la acción automáticamente.**
 - **Bloquear descarga.**
 - **Autorizar descarga.**
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Análisis de Antivirus Internet de direcciones URL con bases de datos de direcciones web fraudulentas y maliciosas

El análisis de enlaces para ver si están incluidos en la lista de direcciones web fraudulentas permite evitar *intentos de fraude*. Un intento de fraude se puede disfrazar, por ejemplo, como un mensaje de correo electrónico de su banco con un enlace al sitio web del banco. Al hacer clic en el enlace, se abre una copia exacta del sitio web del banco e incluso puede ver la dirección real en el navegador, a pesar de que se trata de una imitación. A partir de este momento, todas sus acciones dentro del sitio son rastreadas y pueden servir para robarle su dinero.

Puesto que los enlaces a los sitios web fraudulentos pueden recibirse no solo en el correo electrónico, sino también en otros recursos, como mensajes ICQ, el componente Antivirus Internet supervisa los intentos de acceder a un sitio web fraudulento en el nivel de tráfico web y bloquea el acceso a dichas ubicaciones. Las listas de direcciones fraudulentas se incluyen en el kit de distribución de Kaspersky Endpoint Security.

Para configurar Antivirus Internet de modo que compruebe las direcciones URL con las de las bases de datos de direcciones fraudulentas y maliciosas:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus Internet**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus Internet.
3. Haga clic en el botón **Configuración**.
Se abre la ventana **Antivirus Internet**.

4. En la ventana **Antivirus Internet**, seleccione la pestaña **General**.

5. Haga lo siguiente:

- Si desea que Antivirus Internet compruebe las direcciones URL con las bases de datos de direcciones web maliciosas, en la sección **Métodos de análisis**, seleccione la casilla de verificación **Comprobar si los enlaces están incluidos en la base de datos de enlaces maliciosos**.
- Si quiere que Antivirus Internet compruebe las direcciones URL con las de las bases de datos de direcciones web fraudulentas, en la sección **Configuración del componente Antifraudes**, seleccione la casilla de verificación **Comprobar si los enlaces están incluidos en la base de datos de enlaces fraudulentos**.

También puede comprobar los enlaces con las bases de datos de reputación de [Kaspersky Security Network](#).

6. Haga clic en **Aceptar**.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Uso del Analizador heurístico con Antivirus Internet

Para configurar el uso del análisis heurístico:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus Internet**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus Internet.
3. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
Se abre la ventana **Antivirus Internet**.
4. Seleccione la pestaña **General**.
5. Si quiere que Antivirus Internet utilice el análisis heurístico para analizar el tráfico web en busca de virus y otro malware, en la sección **Métodos de análisis**, seleccione la casilla de verificación **Análisis heurístico para la detección de virus** y utilice el control deslizante para ajustar el nivel de detalle del análisis heurístico: **Análisis superficial**, **Análisis medio** o **Análisis avanzado**.
6. Si desea que Antivirus Internet use el análisis heurístico para analizar páginas web en busca de enlaces de phishing, en la sección **Configuración del componente Antifraudes**, seleccione la casilla de verificación **Análisis heurístico para detectar enlaces fraudulentos**.
7. Haga clic en **Aceptar**.
8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Modificación de la lista de direcciones URL de confianza

Para crear una lista de direcciones URL de confianza:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus Internet**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus Internet.
3. Haga clic en el botón **Configuración**.
Se abre la ventana **Antivirus Internet**.
4. Seleccione la pestaña **Direcciones URL de confianza**
5. Seleccione la casilla **No analizar tráfico Web de direcciones Web de confianza**.
6. Cree una lista de direcciones URL/páginas web en cuyo contenido confíe. Para crear una lista:
 - a. Haga clic en el botón **Agregar**.
Se abre la ventana **Dirección web / Máscara de dirección web**.
 - b. Introduzca la dirección del sitio web/página web o la máscara de dirección del sitio web/página web.
 - c. Haga clic en **Aceptar**.
Aparece un registro nuevo en la lista de direcciones URL de confianza.
7. Haga clic en **Aceptar**.
8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Protección del tráfico de clientes de MI. Antivirus para chat

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security se instala en un equipo con [Microsoft Windows para servidores de archivos](#).

Esta sección contiene información sobre Antivirus para chat e instrucciones sobre cómo configurar los parámetros del componente.

Acerca de Antivirus para chat

Antivirus para chat analiza el tráfico de los *clientes de mensajería instantánea*.

Antivirus para chat no analiza los mensajes transmitidos sobre canales cifrados.

Los mensajes enviados a través de clientes de MI pueden contener los siguientes tipos de amenazas para la seguridad:

- Direcciones URL que intentan descargar un programa malicioso en el equipo
- Direcciones URL de programas maliciosos y sitios web que los intrusos utilizan para ataques fraudulentos
El objetivo de los ataques fraudulentos es robar datos personales del usuario, tales como números de tarjetas bancarias, los datos del pasaporte, contraseñas para sistemas de pagos bancarios y otros servicios en línea (tales como sitios de redes sociales o cuentas de correo electrónico).

Archivos que se pueden transmitir a través de clientes de MI. Cuando se intenta guardar dichos archivos, el componente [Antivirus de archivos](#) los analiza.

Antivirus para chat intercepta cada uno de los mensajes que el usuario envía o recibe a través de un cliente de mensajería instantánea y analiza si hay enlaces que amenacen la seguridad del equipo:

- Si no se detectan URL peligrosas en el mensaje, pasa a estar disponible para el usuario.
- Si se detectan enlaces peligrosos en el mensaje, Antivirus para chat sustituye el mensaje por información sobre la amenaza en la ventana de mensajes del programa de mensajería instantánea activo.





Activación y desactivación del Antivirus para chat

De forma predeterminada, Antivirus para chat está activado, ejecutándose en el modo recomendado por los expertos de Kaspersky. Si es necesario, puede desactivar el Antivirus para chat.

Existen dos formas de activar o desactivar el componente:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

Para activar o desactivar Antivirus para chat en la pestaña Protección y control de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Protección**.
Se abre la sección **Protección**.
4. Haga clic con el botón derecho en la línea **Antivirus para chat** para que se muestre el menú contextual de las acciones del componente.
5. Realice una de las siguientes acciones:
 - Para activar Antivirus para chat, seleccione **Iniciar** en el menú contextual.
El icono de estado del componente , que se muestra a la izquierda en la línea **Antivirus para chat**, cambia al icono .
 - Para desactivar Antivirus para chat, seleccione **Detener** en el menú contextual.
El icono de estado del componente , que se muestra a la izquierda en la línea **Antivirus para chat**, cambia al icono .

Para activar o desactivar Antivirus para chat en la ventana de configuración de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus para chat**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus para chat.
3. Realice una de las siguientes acciones:
 - Si quiere activar Antivirus para chat, seleccione la casilla de verificación **Activar Antivirus para chat**.
 - Si quiere desactivar el Antivirus para chat, desactive la casilla de verificación **Activar Antivirus para chat**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Configuración de Antivirus para chat

Puede llevar a cabo las siguientes acciones para configurar Antivirus para chat:

- Configurar la cobertura de protección.
Puede ampliar o reducir la cobertura de protección modificando el tipo de mensajes del cliente de MI que se analizan.
- Configurar Antivirus para chat para que analice enlaces en mensajes de clientes de mensajería instantánea por medio de bases de datos de direcciones web maliciosas y fraudulentas.

Creación de la Cobertura de protección del Antivirus para chat

La cobertura de protección hace referencia a los objetos que analiza el componente cuando está activado. Las coberturas de protección de los distintos componentes tienen distintas propiedades. El tipo de mensajes de clientes de MI analizados, entrantes o salientes, es una propiedad de la cobertura de Protección antivirus para chat. De forma predeterminada, Antivirus para chat analiza tanto los mensajes entrantes como los salientes. Puede desactivar el análisis del tráfico de salida.

Para crear la Cobertura de protección:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus para chat**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus para chat.
3. En la sección de **Cobertura de protección**, lleve a cabo una de las siguientes acciones:
 - Si quiere que Antivirus para chat analice todos los mensajes de clientes de mensajería instantánea, tanto entrantes como salientes, seleccione la opción **Mensajes entrantes y salientes**.
 - Si quiere que Antivirus para chat solo analice los mensajes entrantes de clientes de mensajería instantánea, seleccione la opción **Solo mensajes entrantes**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Análisis de direcciones URL con bases de datos de direcciones URL maliciosas y fraudulentas con Antivirus para chat

Para configurar Antivirus para chat de modo que compruebe las direcciones URL con las de las bases de datos de direcciones web maliciosas y fraudulentas:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Antivirus para chat**.
En la parte derecha de la ventana se muestra la configuración del componente Antivirus para chat.
3. En la sección **Métodos de análisis**, seleccione los métodos que quiere que use Antivirus para chat:
 - Si desea comprobar los enlaces en los mensajes del cliente de mensajería instantánea con la base de datos de enlaces maliciosos, seleccione la casilla de verificación **Comprobar si los enlaces están incluidos en la base de datos de enlaces maliciosos**.
 - Si desea comprobar los enlaces en los mensajes del cliente de mensajería instantánea con la base de datos de direcciones web fraudulentas, seleccione la casilla de verificación **Comprobar si los enlaces están incluidos en la base de datos de enlaces fraudulentos**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

System Watcher

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security se instala en un equipo con [Microsoft Windows para servidores de archivos](#).

Esta sección contiene información sobre System Watcher e instrucciones sobre cómo configurar los parámetros del componente.

Acerca de System Watcher

System Watcher recopila datos sobre las acciones de las aplicaciones de su equipo y pasa esta información a otros componentes para proporcionar una protección más fiable.

Bases de datos de reglas heurísticas

La tecnología de BSS (Behavior Stream Signatures), también conocida como "Bases de datos de reglas heurísticas", contiene secuencias de acciones de aplicación clasificadas por Kaspersky Endpoint Security como peligrosas. Si la actividad de la aplicación coincide con una base de datos de reglas heurísticas, Kaspersky Endpoint Security realiza la acción especificada. La función de Kaspersky Endpoint Security basada en bases de datos de reglas heurísticas ofrece protección proactiva al equipo.

De forma predeterminada, si la actividad de la aplicación coincide con una base de datos de reglas heurísticas, System Watcher mueve el archivo ejecutable de dicha aplicación a [Cuarentena](#).

Anulación de acciones ejecutadas por un software malicioso (malware)

En función de la información recopilada por System Watcher, Kaspersky Endpoint Security [puede deshacer las acciones ejecutadas en el sistema operativo por un software malicioso](#)  mientras lleva a cabo la desinfección.

Al deshacer la actividad de software malicioso (malware) en el sistema operativo, Kaspersky Endpoint Security realiza acciones sobre los siguientes tipos de actividad de software malicioso:

- Actividad de archivos.

Kaspersky Endpoint Security elimina los archivos ejecutables creados por programas maliciosos y que se encuentren en cualquier soporte, menos en los soportes de red.

Kaspersky Endpoint Security elimina los archivos ejecutables creados por programas en los que hayan penetrado programas maliciosos.

Kaspersky Endpoint Security no restaura archivos modificados ni eliminados.

- Actividad del registro.

Kaspersky Endpoint Security elimina las particiones y las claves de registro creadas por el software malicioso (malware).

Kaspersky Endpoint Security no restaura particiones modificadas ni eliminadas, ni claves de registro.

- Actividad del sistema.

Kaspersky Endpoint Security finaliza procesos iniciados por un programa malicioso.

Kaspersky Endpoint Security finaliza procesos en los que haya penetrado un programa malicioso.

Kaspersky Endpoint Security no reanuda procesos interrumpidos por un programa malicioso.

- Actividad de red.

Kaspersky Endpoint Security bloquea la actividad de red de programas maliciosos.

Kaspersky Endpoint Security bloquea la actividad de red de los procesos en los que ha penetrado un programa malicioso.

La anulación de las acciones de un malware se puede iniciar por parte del [Antivirus de archivos](#), o bien durante un [análisis antivirus](#).

Deshacer las operaciones de un software malicioso (malware) afecta a un conjunto de datos definidos rigurosamente. La anulación no tiene efectos adversos en el sistema operativo ni en la integridad de los datos del equipo.

Activación y desactivación de System Watcher





De forma predeterminada, System Watcher está activado y se ejecuta en el modo que recomienda Kaspersky. Si es necesario, puede desactivar System Watcher.

No se recomienda desactivar System Watcher a menos que sea absolutamente necesario, ya que afecta al rendimiento de los componentes de protección. Los componentes de protección pueden solicitar los datos recopilados por System Watcher para identificar una amenaza detectada con mayor precisión.

Existen dos formas de activar o desactivar System Watcher:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

Para activar o desactivar System Watcher en la pestaña **Protección y control** de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Protección**.
Se abre la sección **Protección**.
4. Haga clic con el botón derecho para mostrar el menú contextual de la línea con información sobre el componente System Watcher.
Se abre un menú para seleccionar acciones sobre los componentes.
5. Realice una de las siguientes acciones:
 - Para activar System Watcher, seleccione **Iniciar**.
El icono de estado del componente , que se muestra a la izquierda en la línea **System Watcher**, cambia al icono .
 - Para desactivar System Watcher, seleccione **Detener**.
El icono de estado del componente , que se muestra a la izquierda en la línea **System Watcher**, cambia al icono .

Para activar o desactivar System Watcher en la ventana de configuración de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **System Watcher**.
En la parte derecha de la ventana, se muestra la configuración del componente **System Watcher**.
3. Realice una de las siguientes acciones:
 - Para activar System Watcher, seleccione la casilla de verificación **Activar System Watcher**.
 - Para desactivar System Watcher, desactive la casilla de verificación **Activar System Watcher**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Configurar System Watcher

Puede realizar las siguientes acciones para configurar System Watcher:

- Activar o desactivar la protección contra exploits;
- elegir una acción en caso de que se detecte actividad maliciosa en un programa;
- Active o desactive la anulación de acciones de malware durante la desinfección.

Activar o desactivar la protección contra exploits

Para activar o desactivar la protección contra [exploits](#):

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **System Watcher**.
En la parte derecha de la ventana, se muestra la configuración del componente **System Watcher**.
3. Realice una de las siguientes acciones:
 - Seleccione la casilla de verificación **Activar Prevención de vulnerabilidades** si quiere que Kaspersky Endpoint Security supervise los archivos utilizados por programas vulnerables cuando se inician.
Si Kaspersky Endpoint Security detecta que un archivo que utiliza un programa vulnerable no fue iniciado por el usuario, actuará de acuerdo con lo que usted seleccionó en la lista emergente **Acción al detectar una amenaza**.
 - Seleccione la casilla de verificación **Activar Prevención de vulnerabilidades** si quiere que Kaspersky Endpoint Security supervise los archivos utilizados por programas vulnerables cuando se inician.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Elija una acción en caso de que se detecte actividad maliciosa en un programa

A fin de elegir qué hacer si un programa participa en actividades maliciosas, realice los pasos siguientes:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **System Watcher**.
En la parte derecha de la ventana, se muestra la configuración del componente **System Watcher**.
3. En la sección **Acción al detectar una amenaza** de la lista emergente **Al detectar actividad de software malicioso**, elija la acción siguiente:
 - **Seleccionar la acción automáticamente.**
 - **Mover archivo a Cuarentena.**
 - **Terminar el software malicioso.**
 - **Omitir.**
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Activación y desactivación de la anulación de acciones de malware durante la desinfección

Para activar o desactivar la anulación de acciones de software malicioso (malware) durante la desinfección:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **System Watcher**.
En la parte derecha de la ventana, se muestra la configuración del componente **System Watcher**.
3. Realice una de las siguientes acciones:
 - Si desea que Kaspersky Endpoint Security deshaga las acciones llevadas a cabo por el software malicioso (malware) en el sistema operativo mientras se realiza la desinfección, seleccione la casilla de verificación **Deshacer acciones de software malicioso durante la desinfección**.
 - Si desea que Kaspersky Endpoint Security ignore las acciones llevadas a cabo por el software malicioso (malware) en el sistema operativo mientras se realiza la desinfección, desactive la casilla de verificación **Deshacer acciones de software malicioso durante la desinfección**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Firewall

Esta sección contiene información sobre Firewall e instrucciones sobre cómo configurar los parámetros del componente.

Acerca de Firewall

Durante su utilización en redes LAN e Internet, un equipo está expuesto a virus, a otro software malicioso (malware) y a diferentes ataques que explotan las vulnerabilidades de los sistemas operativos y el software.

El firewall protege los datos personales que se almacenan en el equipo del usuario, bloqueando la mayor cantidad posible de amenazas al sistema operativo mientras que el equipo está conectado a Internet o a una red de área local. Firewall detecta todas las conexiones de red del equipo del usuario y proporciona una lista de direcciones IP, con una indicación del estado de la conexión de red predeterminada.

El componente Firewall filtra toda la actividad de red según las [Reglas de la red](#). La configuración de las reglas de red permite especificar el nivel deseado para la protección del equipo, desde el bloqueo del acceso a Internet para todas las aplicaciones hasta el acceso ilimitado.





Activación y desactivación de Firewall

De forma predeterminada, Firewall está activado y las opciones en el modo óptimo. Si fuera necesario, puede desactivar Firewall.

Existen dos formas de activar o desactivar el componente:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

Para activar o desactivar Firewall en la pestaña Protección y control de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Protección**.
Se abre la sección **Protección**.
4. Haga clic con el botón derecho del ratón en la línea **Firewall** para abrir el menú contextual de acciones de Firewall.
5. Realice una de las siguientes acciones:
 - Para activar Firewall, en el menú contextual, seleccione **Iniciar**.
El icono de estado del componente , que se muestra a la izquierda en la línea **Firewall**, cambia al icono .
 - Para desactivar Firewall, seleccione **Detener** en el menú contextual.
El icono de estado del componente , que se muestra a la izquierda en la línea **Firewall**, cambia al icono .

Para activar o desactivar Firewall, en la ventana de configuración de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Firewall**.
En la parte derecha de la ventana se muestra la configuración del componente Firewall.
3. Realice una de las siguientes acciones:
 - Para activar Firewall, seleccione la casilla de verificación **Activar Firewall**.
 - Para desactivar Firewall, seleccione la casilla de verificación **Activar Firewall**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Acerca de las reglas de red

Reglas de la red son acciones permitidas o bloqueadas que lleva a cabo el componente Firewall al detectar un intento de conexión de red.

Firewall proporciona protección contra ataques de red de distintos tipos en dos niveles: el nivel de red y el nivel de programa. La protección en el nivel de red se proporciona aplicando reglas de paquetes de red. La protección en el nivel de programas se proporciona aplicando reglas en función de las cuales las aplicaciones instaladas pueden acceder a los recursos de red.

Basándose en los dos niveles de protección de Firewall, puede crear lo siguiente:

- *Reglas de paquetes de red*. Las reglas de paquetes de red imponen restricciones a los paquetes de red, con independencia del programa. Estas reglas restringen el tráfico de red entrante y saliente a través de puertos específicos del protocolo de datos seleccionado. Firewall especifica determinadas reglas de paquetes de red de forma predeterminada.
- *Reglas de red de la aplicación*. Las reglas de red de la aplicación imponen restricciones sobre la actividad de red de una aplicación concreta. No solo influyen en las características del paquete de red, sino también en la aplicación concreta a la que va dirigida la aplicación concreta o que emitió este paquete de red. Estas reglas permiten ajustar mejor el filtrado de la actividad de red: por ejemplo, cuando un tipo determinado de conexión de red está bloqueado para algunas aplicaciones, pero está permitido para otras.

Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones. Si tanto las reglas de paquetes de red como las reglas de red para aplicaciones se especifican para el mismo tipo de actividad de red, la actividad de red se gestiona de acuerdo con las reglas de paquetes de red.

Puede especificar una prioridad de ejecución para cada regla de paquetes de red y cada regla de red para aplicaciones.

Las reglas de paquetes de red tienen prioridad sobre las reglas de red para aplicaciones. Si tanto las reglas de paquetes de red como las reglas de red para aplicaciones se especifican para el mismo tipo de actividad de red, la actividad de red se gestiona de acuerdo con las reglas de paquetes de red.

Las reglas de red para aplicaciones funcionan de la siguiente manera: una regla de red para aplicaciones incluye reglas de acceso basadas en el estado de la red: *pública*, *local* o *de confianza*. Por ejemplo, a las aplicaciones del grupo de confianza Restricción máxima se les niega cualquier actividad de red en redes de cualquier estado de forma predeterminada. Si se especifica una regla de red para una aplicación individual (aplicación principal), los subprocesos de otras aplicaciones se ejecutarán de acuerdo con la regla de red de la aplicación principal. Si no hay una regla de red para la aplicación, los subprocesos se ejecutarán de acuerdo con la regla de acceso a la red del grupo de confianza de la aplicación.

Por ejemplo, ha prohibido cualquier actividad de red en redes de todos los estados para todas las aplicaciones, excepto el navegador X. Si inicia la instalación del navegador Y (subproceso) desde el navegador X (aplicación principal), el instalador del navegador Y accederá a la red y descargará los archivos necesarios. Después de la instalación, se negarán las conexiones de red al navegador Y de acuerdo con la configuración del Firewall. Para prohibir la actividad de red del instalador del navegador Y como un subproceso, debe asignar una regla de red para el instalador del navegador Y.

Acerca del estado de la conexión de red

Firewall controla todas las conexiones de red del equipo del usuario y asigna automáticamente un estado a cada conexión de red que detecte.

La conexión de red puede tener uno de los siguientes tipos de estado:

- **Red pública.** Este estado es para redes que no están protegidas por ninguna aplicación antivirus, firewall o filtro (por ejemplo, las redes de los cibercafés). Cuando el usuario utiliza un equipo conectado a una red de este tipo, Firewall bloquea el acceso a los archivos e impresoras de este equipo. Los usuarios externos tampoco pueden acceder a los datos mediante carpetas compartidas y acceso remoto al escritorio de este equipo. Firewall filtra la actividad de red de cada aplicación según las reglas de red establecidas para ella.

Firewall asigna el estado *Red pública* a Internet de forma predeterminada. No se puede cambiar el estado de Internet.

- **Red local.** Este estado se asigna a las redes cuyos usuarios son de confianza para acceder a los archivos e impresoras de este equipo (por ejemplo, una red LAN o doméstica).
- **Red de confianza.** Este estado está pensado para una red segura en la que el equipo no está expuesto a ataques o intentos de acceso a datos no autorizados. Firewall permite cualquier actividad de red dentro de redes con este estado.

Modificación del estado de la conexión de red

Para cambiar el estado de la conexión de red:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección Antivirus**, seleccione el apartado **Firewall**.
En la parte derecha de la ventana se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Redes disponibles**.
Se abre la ventana **Firewall**.
4. Seleccione la conexión de red cuyo estado quiere cambiar.
5. En el menú contextual, seleccione [el estado de la conexión de red](#):
 - **Red pública.**
 - **Red local.**
 - **Red de confianza.**
6. En la ventana **Firewall**, haga clic en **Aceptar**.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Gestión de las reglas de paquetes de red

Puede realizar las siguientes acciones mientras gestiona las reglas de paquetes de red:

- Crear una nueva regla de paquetes de red.

Puede crear una nueva regla de paquetes de red mediante la creación de un conjunto de condiciones y acciones que se aplican a los paquetes de red y los flujos de datos.

- Activar o desactivar una regla de paquetes de red.

Todas las reglas de paquetes de red creadas por Firewall tienen el estado *Activado* de forma predeterminada. Cuando una regla de paquetes de red está activada, Firewall aplica esta regla.

Puede desactivar cualquier regla de paquetes de red que esté seleccionada en la lista de reglas de paquetes de red. Cuando una regla de paquetes de red está desactivada, Firewall deja de aplicar temporalmente esta regla.

Con el estado *Activado*, se añade de forma predeterminada una nueva regla de paquetes de red personalizada a la lista de reglas de paquetes de red.

- Modificar los parámetros de una regla de paquetes de red ya existente.

Tras crear una nueva regla de paquetes de red, siempre puede volver a modificar sus parámetros y modificarlos si es necesario.

- Cambiar la acción de Firewall para una regla de paquetes de red.

En la lista de reglas de paquetes de red, puede modificar la acción que Firewall realiza para detectar la actividad de red que cumple con una regla de paquetes de red concreta.

- Cambiar la prioridad de una regla de paquetes de red.

Puede incrementar o reducir la prioridad de una regla de paquetes de red que esté seleccionada en la lista.

- Eliminar una regla de paquetes de red.

Puede eliminar una regla de paquetes de red para que Firewall deje de aplicar esta regla cuando detecte actividad de red y para que esta regla no se muestre en la lista de reglas de paquetes de red con el estado *Desactivado*.

Creación y edición de una regla de paquetes de red

Al crear reglas de paquetes de red, recuerde que estas tienen prioridad sobre las reglas para aplicaciones.

Para crear o editar una regla de paquetes de red:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Firewall**.

3. Haga clic en el botón **Reglas de paquetes de red**.

4. Se abre la ventana **Firewall** en la pestaña **Reglas de paquetes de red**.

Esta pestaña muestra una lista de reglas de paquetes de red predeterminadas definidas por el componente Firewall.

5. Realice una de las siguientes acciones:


- Para crear una nueva regla de paquetes de red, haga clic en el botón **Agregar**.
- Para editar una regla de paquetes de red, selecciónela en la lista de reglas de paquetes de red y haga clic en el botón **Modificar**.

Se abre la ventana **Regla de la red**.

6. En la lista desplegable **Acción**, seleccione la acción que debe realizar Firewall cuando detecte este tipo de actividad de red:

- **Autorizar**
- **Bloquear**
- **Por reglas de la aplicación.**

7. En el campo **Nombre**, especifique el nombre del [servicio de red](#) de una de las siguientes formas:

- Haga clic en el icono  a la derecha del campo **Nombre** y seleccione el nombre del servicio de red en la lista desplegable.
La lista desplegable incluye servicios de red que definen las conexiones de red utilizadas con más frecuencia.
- Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.

8. Especifique el protocolo de transferencia de datos:

a. Seleccione la casilla de verificación **Protocolo**.

b. En la lista desplegable, seleccione el tipo de protocolo para el que se debe supervisar la actividad de red.

Firewall supervisa las conexiones de red que utilizan los protocolos TCP, UDP, ICMP, ICMPv6, IGMP y GRE.

Si selecciona un servicio de red de la lista desplegable **Nombre**, la casilla de verificación **Protocolo** se selecciona de forma automática y la lista desplegable situada junto a la casilla de verificación contiene el tipo de protocolo correspondiente al servicio de red seleccionado. De forma predeterminada, la casilla de verificación **Protocolo** está desactivada.

9. En la lista desplegable **Dirección**, seleccione la dirección de la actividad de red supervisada.

Firewall supervisa las conexiones de red con las direcciones siguientes:

- **Entrante (paquete).**
- **Entrante.**
- **Entrante/Saliente**
- **Saliente (paquete).**
- **Saliente.**

10. Si ICMP o ICMPv6 se selecciona como el protocolo, puede especificar el código y el tipo de paquete ICMP:
- Seleccione la casilla de verificación **Tipo de ICMP** y seleccione el tipo de paquete ICMP en la lista desplegable.
 - Seleccione la casilla de verificación **Código ICMP** y seleccione el código de paquete ICMP en la lista desplegable.
11. Si se selecciona TCP o UDP como tipo de protocolo, puede especificar los números de puerto delimitados por comas de los equipos local y remoto entre los que se debe supervisar la conexión:
- Introduzca los puertos del equipo remoto en el campo **Puertos remotos**.
 - Introduzca los puertos del equipo remoto en el campo **Puertos locales**.
12. En la tabla **Adaptadores de red**, especifique la configuración de los adaptadores de red desde los cuales se pueden enviar los paquetes de red o que pueden recibir paquetes de red. Para ello, utilice los botones **Agregar**, **Editar** y **Eliminar**.
13. Si desea restringir el control de paquetes de red según su período de vida (TTL, por sus siglas en inglés), seleccione la casilla de verificación **TTL** y, en el campo que hay junto a ella, especifique el intervalo de valores del período de vida para los paquetes de red entrantes y salientes.
- Una regla de red controlará la transmisión de los paquetes de red cuyo período de vida no supere el valor especificado.
- De lo contrario, desactive la casilla de verificación **TTL**.
14. Especifique las direcciones de red de los equipos remotos que puedan enviar o recibir paquetes de red. Para ello, seleccione uno de los valores siguientes en la lista desplegable **Direcciones remotas**:
- **Cualquier dirección.** La regla de red controla los paquetes de red que hayan enviado o recibido los equipos remotos con cualquier dirección IP.
 - **Direcciones de subred.** La regla de red controla los paquetes de red enviados y recibidos por equipos remotos con direcciones IP asociadas al tipo de la red seleccionado: **Redes de confianza**, **Redes locales** o **Redes públicas**.
 - **Direcciones de la lista.** La regla de red controla los paquetes de red que hayan enviado o recibido los equipos remotos con direcciones IP que se puedan especificar en la lista que se muestra debajo a través de los botones **Agregar**, **Modificar** y **Eliminar**.
15. Especifique las direcciones de red de los equipos que cuentan con Kaspersky Endpoint Security instalada, y pueden enviar y recibir paquetes de red. Para ello, seleccione uno de los valores siguientes en la lista desplegable **Direcciones locales**:
- **Cualquier dirección.** La regla de red controla los paquetes de red que hayan enviado o recibido los equipos remotos con cualquier dirección IP que tengan instalado Kaspersky Endpoint Security.
 - **Direcciones de la lista.** La regla de red controla los paquetes de red que hayan enviado o recibido los equipos remotos que tengan instalado Kaspersky Endpoint Security con direcciones IP que se puedan especificar en la lista que se muestra debajo a través de los botones **Agregar**, **Modificar** y **Eliminar**.

En ocasiones, no se puede obtener una dirección local para aplicaciones que funcionan con paquetes de red. Si es este el caso, se ignora el valor del parámetro **Direcciones locales**.

16. Si desea que las acciones de la regla de la red se reflejen en el [informe](#), seleccione la casilla de verificación **Registrar eventos**.
17. En la ventana **Regla de red**, haga clic en **Aceptar**.
Si crea una nueva regla de red, la regla se muestra en la pestaña **Reglas de paquetes de red** de la ventana **Firewall**. De forma predeterminada, la nueva regla de red se coloca al final de la lista de reglas de paquetes de red.
18. En la ventana **Firewall**, haga clic en **Aceptar**.
19. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Activación o desactivación de una regla de paquetes de red

Para activar o desactivar una regla de paquetes de red:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección Antivirus**, seleccione el apartado **Firewall**.
En la parte derecha de la ventana se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Reglas de paquetes de red**.
Se abre la ventana **Firewall** en la pestaña **Reglas de paquetes de red**.
4. Seleccione la regla de los paquetes de red pertinente en la lista.
5. Realice una de las siguientes acciones:
 - Para activar la regla, seleccione la casilla de verificación junto al nombre de la regla de paquetes de red.
 - Para desactivar la regla, desactive la casilla de verificación junto al nombre de la regla de paquetes de red.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Modificación de la acción de Firewall para una regla de paquetes de red

Para cambiar la acción de Firewall que se aplica a una regla de paquetes de red:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección Antivirus**, seleccione el apartado **Firewall**.
En la parte derecha de la ventana se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Reglas de paquetes de red**.
Se abre la ventana **Firewall** en la pestaña **Reglas de paquetes de red**.
4. En la lista, seleccione la regla de paquetes de red cuya acción quiere cambiar.

5. En la columna **Permiso**, haga clic con el botón derecho para acceder al menú contextual y seleccione la acción que quiere asignar:

- **Autorizar**
- **Bloquear**
- **De acuerdo con la regla para la aplicación**
- **Registrar eventos**

6. En la ventana **Firewall**, haga clic en **Aceptar**.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Modificación de la prioridad de una regla de paquetes de red

La prioridad de una regla de paquetes de red viene determinada por su posición en la lista de reglas de paquetes de red. La regla de paquetes de red situada más arriba en la lista de reglas de paquetes de red tiene la máxima prioridad.

Cada una de las reglas de paquetes de red creadas manualmente se agrega al final de la lista de reglas de paquetes de red y tienen la menor prioridad.

Firewall ejecuta las reglas en el orden en que aparecen en la lista de reglas de paquetes de red, de arriba abajo. En función de cada una de las reglas de paquetes de red procesadas que se aplican a una determinada conexión de red, Firewall permite o bloquea el acceso de red a la dirección y al puerto especificados en la configuración de esta conexión de red.

Para modificar la prioridad de la regla de paquetes de red:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección Antivirus**, seleccione el apartado **Firewall**.
En la parte derecha de la ventana se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Reglas de paquetes de red**.
Se abre la ventana **Firewall** en la pestaña **Reglas de paquetes de red**.
4. En la lista, seleccione la regla de paquetes de red cuya prioridad quiere cambiar.
5. Utilice los botones **Subir** y **Bajar** para mover la regla de paquetes de red al punto que desee en la lista de reglas de paquetes de red.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Gestionar reglas de red de la aplicación

De forma predeterminada, Kaspersky Endpoint Security agrupa todas las aplicaciones que están instaladas en el equipo por el nombre del proveedor del software cuyo archivo o actividad de red monitoriza. Los grupos de aplicaciones, a su vez, se clasifican en [grupos de confianza](#). Todas las aplicaciones y grupos de aplicaciones heredan las propiedades de su grupo principal: reglas de control de aplicaciones, reglas de red de la aplicación y su prioridad de ejecución.

De forma predeterminada, el componente Firewall aplica las reglas de red a un grupo de aplicaciones cuando filtra la actividad de red de todas las aplicaciones dentro del grupo, de modo similar al componente [Control de actividad de aplicaciones](#). El grupo de aplicaciones define los derechos de las aplicaciones dentro del grupo a acceder a diferentes conexiones de red.

De forma predeterminada, Firewall crea un conjunto de reglas de red para cada grupo de aplicaciones que Kaspersky Endpoint Security detecta en el equipo. Puede cambiar la acción que Firewall aplica a las reglas de red del grupo de aplicaciones que se crean de forma predeterminada. No puede modificar, eliminar, desactivar o cambiar la prioridad de las reglas de red del grupo de aplicaciones que se crean de forma predeterminada.

También puede crear una regla de red para una aplicación individual. Tal regla tendrá una prioridad más alta que la regla de red del grupo al cual la aplicación pertenece.

Puede realizar las siguientes acciones mientras gestiona las reglas de red de la aplicación:

- Cree una nueva regla de red.

Puede crear una nueva regla de red por la cual el Firewall debe regular la actividad de red de la aplicación o las aplicaciones que pertenecen al grupo de aplicaciones seleccionado.

- Active o desactive una regla de red.

Todas las reglas de red se agregan a la lista de reglas de red de aplicaciones con el estado *Activado*. Si una regla de red está activada, Firewall aplica esta regla.

Puede desactivar una regla de red que se creó manualmente. Cuando una regla de red está desactivada, Firewall deja de aplicar temporalmente esta regla.

- Cambie los ajustes de una regla de red.

Tras crear una nueva regla de red, siempre puede volver a editar sus ajustes y modificarlos si es necesario.

- Cambie la acción de Firewall para una regla de red.

En la lista de reglas de red, puede editar la acción que Firewall aplica para la regla de red al detectar actividad de red en esta aplicación o grupo de aplicaciones.

- Cambie la prioridad de una regla de red.

Puede incrementar o reducir la prioridad de una regla de red personalizada.

- Elimine una regla de red.

Puede eliminar una regla de red personalizada a fin de que Firewall deje de aplicar esta regla de red a la aplicación seleccionada cuando detecte actividad de red y para que esta regla no se muestre en la lista de reglas de red de la aplicación.

Creación y edición de una regla de red para una aplicación

Para crear y editar una regla de red para un grupo de aplicaciones:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Protección Antivirus**, seleccione el apartado **Firewall**.

3. Haga clic en el botón **Reglas de red de la aplicación**.

Se abre la ventana **Firewall** en la pestaña **Reglas de Control de aplicaciones**.

4. En la lista de aplicaciones, seleccione la aplicación o el grupo de aplicaciones para el que quiere crear o editar una regla de red.

5. Haga clic con el botón derecho del ratón para acceder al menú contextual y seleccione **Reglas de la aplicación** o **Reglas del grupo** según lo que precise hacer.

Esto abre la ventana **Reglas de Control de aplicaciones/Reglas de control de grupos de aplicaciones**.

6. En la ventana de diálogo que se abre, seleccione la pestaña **Reglas de la red**.

7. Realice una de las siguientes acciones:


- Para crear una nueva regla de la red, haga clic en el botón **Agregar**.
- Para editar una regla de la red, selecciónela en la lista de reglas de la red y haga clic en el botón **Editar**.

Se abre la ventana **Regla de la red**.

8. En la lista desplegable **Acción**, seleccione la acción que debe realizar Firewall cuando detecte este tipo de actividad de red:

- **Autorizar**
- **Bloquear**

9. En el campo **Nombre**, especifique el nombre del [servicio de red](#) de una de las siguientes formas:

- Haga clic en el icono  a la derecha del campo **Nombre** y seleccione el nombre del servicio de red en la lista desplegable.
La lista desplegable incluye servicios de red que definen las conexiones de red utilizadas con más frecuencia.
- Introduzca manualmente el nombre del servicio de red en el campo **Nombre**.

10. Especifique el protocolo de transferencia de datos:

a. Seleccione la casilla de verificación **Protocolo**.

b. En la lista desplegable, seleccione el tipo de protocolo en el que supervisar la actividad de red.

Firewall supervisa las conexiones de red que utilizan los protocolos TCP, UDP, ICMP, ICMPv6, IGMP y GRE.

Si selecciona un servicio de red de la lista desplegable **Nombre**, la casilla de verificación **Protocolo** se selecciona de forma automática y la lista desplegable situada junto a la casilla de verificación contiene el tipo de protocolo correspondiente al servicio de red seleccionado. De forma predeterminada, la casilla de verificación **Protocolo** está desactivada.

11. En la lista desplegable **Dirección**, seleccione la dirección de la actividad de red supervisada.

Firewall supervisa las conexiones de red con las direcciones siguientes:

- **Entrante**.

- **Entrante/Saliente.**

- **Saliente.**

12. Si ICMP o ICMPv6 se selecciona como el protocolo, puede especificar el código y el tipo de paquete ICMP:

- a. Seleccione la casilla de verificación **Tipo de ICMP** y seleccione el tipo de paquete ICMP en la lista desplegable.
- b. Seleccione la casilla de verificación **Código ICMP** y seleccione el código de paquete ICMP en la lista desplegable.

13. Si se selecciona TCP o UDP como tipo de protocolo, puede especificar los números de puerto delimitados por comas de los equipos local y remoto entre los que se debe supervisar la conexión:

- a. Introduzca los puertos del equipo remoto en el campo **Puertos remotos**.
- b. Introduzca los puertos del equipo local en el campo **Puertos locales**.

14. Especifique las direcciones de red de los equipos remotos que puedan enviar o recibir paquetes de red. Para ello, seleccione uno de los valores siguientes en la lista desplegable **Direcciones remotas**:

- **Cualquier dirección.** La regla de red controla los paquetes de red que hayan enviado o recibido los equipos remotos con cualquier dirección IP.
- **Direcciones de subred.** La regla de red controla los paquetes de red enviados y recibidos por equipos remotos con direcciones IP asociadas al tipo de la red seleccionado: **Redes de confianza, Redes locales o Redes públicas.**
- **Direcciones de la lista.** La regla de red controla los paquetes de red que hayan enviado o recibido los equipos remotos con direcciones IP que se puedan especificar en la lista que se muestra debajo a través de los botones **Agregar, Modificar y Eliminar**.

15. Especifique las direcciones de red de los equipos que cuentan con Kaspersky Endpoint Security instalada, y pueden enviar y recibir paquetes de red. Para ello, seleccione uno de los valores siguientes en la lista desplegable **Direcciones locales**:

- **Cualquier dirección.** La regla de red controla los paquetes de red que hayan enviado o recibido los equipos remotos con cualquier dirección IP que tengan instalado Kaspersky Endpoint Security.
- **Direcciones de la lista.** La regla de red controla los paquetes de red que hayan enviado o recibido los equipos remotos que tengan instalado Kaspersky Endpoint Security con direcciones IP que se puedan especificar en la lista que se muestra debajo a través de los botones **Agregar, Modificar y Eliminar**.

En ocasiones, no se puede obtener una dirección local para aplicaciones que funcionan con paquetes de red. Si es este el caso, se ignora el valor del parámetro **Direcciones locales**.

16. Si desea que las acciones de la regla de la red se reflejen en el [informe](#), seleccione la casilla de verificación **Registrar eventos**.

17. En la ventana **Regla de red**, haga clic en **Aceptar**.

Si creó una nueva regla de la red, la regla se muestra en la pestaña **Reglas de la red**.

18. Haga clic en **Aceptar** en la ventana **Reglas de control de grupos de aplicaciones** si la regla está pensada para un grupo de aplicaciones, o bien en la ventana **Reglas de Control de aplicaciones** si la regla está pensada para

una aplicación.

19. En la ventana **Firewall**, haga clic en **Aceptar**.

20. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Activar y desactivar una regla de red de la aplicación

Para activar o desactivar una regla de red de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Protección Antivirus**, seleccione el apartado **Firewall**.
En la parte derecha de la ventana se muestra la configuración del componente Firewall.

3. Haga clic en el botón **Reglas de red de la aplicación**.

Se abre la ventana **Firewall** en la pestaña **Reglas de Control de aplicaciones**.

4. En la lista, seleccione el grupo de aplicaciones para el que quiere activar o desactivar una regla de red.

5. Haga clic con el botón derecho del ratón para acceder al menú contextual y seleccione **Reglas de la aplicación** o **Reglas del grupo** según lo que precise hacer.

Esto abre la ventana **Reglas de Control de aplicaciones/Reglas de control de grupos de aplicaciones**.

6. En la ventana de diálogo que se abre, seleccione la pestaña **Reglas de la red**.

7. En la lista de reglas de red para un grupo de aplicaciones, seleccione la regla de red pertinente.

8. Realice una de las siguientes acciones:

- Si desea activar la regla, seleccione la casilla de verificación junto al nombre de la regla de red.
- Si desea desactivar la regla, desactive la casilla de verificación junto al nombre de la regla de red.

No puede desactivar una regla de red del grupo de aplicaciones que Firewall haya creado de forma predeterminada.

9. Haga clic en **Aceptar** en la ventana **Reglas de control de grupos de aplicaciones** si la regla está pensada para un grupo de aplicaciones, o bien en la ventana **Reglas de Control de aplicaciones** si la regla está pensada para una aplicación.

10. En la ventana **Firewall**, haga clic en **Aceptar**.

11. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Modificación de la acción de Firewall para una regla de red de la aplicación

Puede cambiar la acción de Firewall que se aplica a las reglas de red para una aplicación o grupo de aplicaciones creado de forma predeterminada y cambiar la acción de Firewall por una única regla de red del grupo de aplicaciones personalizada.

Para cambiar la acción del Firewall sobre todas las reglas de red para una aplicación o grupo de aplicaciones:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección Antivirus**, seleccione el apartado **Firewall**.
En la parte derecha de la ventana se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Reglas de red de la aplicación**.
Se abre la ventana **Firewall** en la pestaña **Reglas de Control de aplicaciones**.
4. Si desea cambiar la acción del Firewall que se aplica a todas las reglas de red que se crean de forma predeterminada, seleccione una aplicación o grupo de aplicaciones de la lista. Las reglas de red creadas manualmente no se cambian.
5. En la columna **Red**, haga clic con el botón derecho para acceder al menú contextual y seleccione la acción que quiere asignar:
 - **Heredar**
 - **Autorizar**
 - **Bloquear**
6. Haga clic en **Aceptar**.
7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Para cambiar la respuesta de Firewall para las reglas de red de una aplicación o un grupo de aplicaciones:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione **Firewall**.
En la parte derecha de la ventana se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Reglas de red de la aplicación**.
Se abre la ventana **Firewall** en la pestaña **Reglas de Control de aplicaciones**.
4. En la lista, seleccione la aplicación o el grupo de aplicaciones para las cuales desea cambiar la acción para una regla de red.
5. Haga clic con el botón derecho del ratón para acceder al menú contextual y seleccione **Reglas de la aplicación** o **Reglas del grupo** según lo que precise hacer.
Esto abre la ventana **Reglas de Control de aplicaciones/Reglas de control de grupos de aplicaciones**.
6. En la ventana de diálogo que se abre, seleccione la pestaña **Reglas de la red**.
7. Seleccione la regla de red para la cual desea cambiar la acción del Firewall.
8. En la columna **Permiso**, haga clic con el botón derecho para acceder al menú contextual y seleccione la acción que quiere asignar:

- **Autorizar**
- **Bloquear**
- **Registrar eventos**

9. Haga clic en **Aceptar** en la ventana **Reglas de control de grupos de aplicaciones** si la regla está pensada para un grupo de aplicaciones, o bien en la ventana **Reglas de Control de aplicaciones** si la regla está pensada para una aplicación.

10. En la ventana **Firewall**, haga clic en **Aceptar**.

11. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Modificación de la prioridad de una regla de red de la aplicación

La prioridad de una regla de red depende de su posición en la lista de reglas. Firewall ejecuta las reglas en el orden en que aparecen en la lista de reglas de red, de arriba abajo. En función de cada una de las reglas de red aplicables a una determinada conexión de red, Firewall permite o bloquea el acceso a la red a la dirección y al puerto indicados en la configuración de esta conexión de red.

Las reglas de red creadas manualmente tienen una prioridad más alta que las reglas de red predeterminadas.

No puede cambiar la prioridad de las reglas de red del grupo de aplicaciones que se crean de forma predeterminada.

Para cambiar la prioridad de una regla de red:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección Antivirus**, seleccione el apartado **Firewall**.
En la parte derecha de la ventana se muestra la configuración del componente Firewall.
3. Haga clic en el botón **Reglas de red de la aplicación**.
Se abre la ventana **Firewall** en la pestaña **Reglas de Control de aplicaciones**.
4. En la lista de aplicaciones, seleccione la aplicación o el grupo de aplicaciones para el que quiere cambiar la prioridad de una regla de red.
5. Haga clic con el botón derecho del ratón para acceder al menú contextual y seleccione **Reglas de la aplicación** o **Reglas del grupo** según lo que precise hacer.
Esto abre la ventana **Reglas de Control de aplicaciones/Reglas de control de grupos de aplicaciones**.
6. En la ventana de diálogo que se abre, seleccione la pestaña **Reglas de la red**.
7. Seleccione la conexión de red cuya prioridad quiera cambiar.
8. Utilice los botones **Subir** y **Bajar** para mover la regla de red al punto que desee en la lista de reglas de red.
9. Haga clic en **Aceptar** en la ventana **Reglas de control de grupos de aplicaciones** si la regla está pensada para un grupo de aplicaciones, o bien en la ventana **Reglas de Control de aplicaciones** si la regla está pensada para

una aplicación.

10. En la ventana **Firewall**, haga clic en **Aceptar**.

11. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Monitor de red

Esta sección contiene información acerca de Monitor de red y las instrucciones sobre cómo iniciar Monitor de red.

Acerca de Monitor de red

Monitor de red es una herramienta diseñada para la visualización de información sobre la actividad de red del equipo de un usuario en tiempo real.

Inicio de Monitor de red

Para iniciar el Monitor de red:

1. Abra la [ventana principal de la aplicación](#).

2. Seleccione la pestaña **Protección y control**.

3. Haga clic en la sección **Protección**.

Se abre la sección **Protección**.

4. Haga clic con el botón derecho en la línea **Firewall** para abrir el menú contextual de las operaciones de Firewall.

5. En el menú contextual, seleccione **Monitor de red**.

Se abre la ventana **Monitor de red**. En esta ventana, se muestra información sobre la actividad de red del equipo en cuatro pestañas:

- La pestaña **Actividad de red** muestra todas las conexiones de red activas actualmente con el equipo. Se indican tanto las conexiones de red salientes como las entrantes.
- La pestaña **Puertos abiertos** muestra todos los puertos de red abiertos del equipo.
- La pestaña **Tráfico de red** muestra el volumen de tráfico de red entrante y saliente entre el equipo del usuario y otros equipos de la red a los que el usuario está conectado actualmente.
- La pestaña **Equipos bloqueados** incluye las direcciones IP de los equipos remotos cuya actividad de red ha bloqueado el componente Prevención de intrusiones después de detectar intentos de ataques de red desde dichas direcciones IP.

Prevención de intrusiones

Esta sección contiene información sobre Prevención de intrusiones, además de instrucciones sobre cómo configurar los parámetros del componente.

Acerca de Prevención de intrusiones

Prevención de intrusiones analiza el tráfico de red entrante en busca de actividad habitual de los ataques de red. Al detectar un intento de ataque de red dirigido a su equipo, Kaspersky Endpoint Security bloquea la actividad de red del equipo atacante. A continuación, su pantalla muestra una advertencia en la que se comunica que se ha producido un intento de ataque y muestra la información sobre el equipo atacante.

El tráfico de red del equipo de ataque se bloquea durante una hora. Puede editar la configuración para bloquear un equipo atacante.

Las bases de datos de Kaspersky Endpoint Security ofrecen descripciones de los tipos de ataques de red actualmente conocidos y los modos para combatirlos. La lista de ataques de red que detecta el componente Prevención de intrusiones se actualiza durante [las actualizaciones de módulos de aplicaciones y bases de datos](#).



Activación y desactivación de Prevención de intrusiones



De forma predeterminada, Prevención de intrusiones está activado, funcionando en modo óptimo. Puede desactivarlo si fuera necesario.

Existen dos formas de activar o desactivar el componente:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

Para activar o desactivar Prevención de intrusiones, haga lo siguiente en la pestaña Protección y control de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Protección**.
Se abre la sección **Protección**.
4. Haga clic con el botón derecho en la línea **Prevención de intrusiones** para mostrar el menú contextual de las acciones de Prevención de intrusiones.
5. Realice una de las siguientes acciones:
 - Para activar Prevención de intrusiones, seleccione **Iniciar** en el menú contextual.
El icono de estado  del componente, que se muestra a la izquierda en la línea **Prevención de intrusiones**, cambiará al icono .
 - Para desactivar Prevención de intrusiones, seleccione **Detener** en el menú contextual.

El icono de estado  del componente, que se muestra a la izquierda en la línea **Prevención de intrusiones**, cambiará al icono .

Para activar o desactivar Prevención de intrusiones en la ventana de configuración de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Prevención de intrusiones**.
La configuración de Prevención de intrusiones se muestra en la parte derecha de la ventana.
3. Haga lo siguiente:
 - Para activar Prevención de intrusiones, seleccione la casilla de verificación **Activar el Sistema de prevención de intrusiones**.
 - Para desactivar Prevención de intrusiones, desactive la casilla de verificación **Activar el Sistema de prevención de intrusiones**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Parámetros de prevención de intrusiones

Puede llevar a cabo las siguientes acciones para configurar los ajustes de Prevención de intrusiones:

- Configure los ajustes utilizados para bloquear un equipo atacante.
- Genere una lista de direcciones de exclusiones de bloqueo.

Edición de la configuración utilizada para bloquear un equipo atacante

Para editar la configuración para el bloqueo de un equipo atacante:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Prevención de intrusiones**.
La configuración de Prevención de intrusiones se muestra en la parte derecha de la ventana.
3. Seleccione la casilla de verificación **Agregar el equipo atacante a la lista de equipos bloqueados durante**.
Si se selecciona esta casilla de verificación, al detectar un intento de ataque de red, Prevención de intrusiones bloquea el tráfico de red desde el equipo atacante durante el tiempo especificado. Esto protege el equipo automáticamente frente a posibles ataques futuros desde la misma dirección.
Si se desactiva la selección de esta casilla de verificación, al detectar un intento de ataque de red, Prevención de intrusiones no activa la protección automática frente a posibles ataques de red futuros desde la misma dirección.
4. Cambie el período de tiempo durante el que se bloquea un equipo atacante en el campo situado junto a la casilla de verificación **Agregar el equipo atacante a la lista de equipos bloqueados durante**.

5. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Configurar direcciones de exclusiones de bloqueo

Para configurar direcciones de exclusiones de bloqueo:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione el apartado **Prevención de intrusiones**.

La configuración de Prevención de intrusiones se muestra en la parte derecha de la ventana.

3. Haga clic en el botón **Exclusiones**.

Se abre la ventana **Exclusiones**.

4. Realice una de las siguientes acciones:

- Si desea crear una nueva dirección IP, haga clic en el botón **Agregar**.
- Si desea editar una dirección IP agregada con anterioridad, selecciónela en la lista de reglas y haga clic en el botón **Editar**.

Se abre la ventana **Dirección IP**.

5. Introduzca la dirección IP del equipo desde el que no se deben bloquear los ataques de red.

6. En la ventana **Dirección IP**, haga clic en **Aceptar**.

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

8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Prevención de ataques de BadUSB

Esta sección contiene información sobre el componente Prevención de ataques de BadUSB.

Acerca de Prevención de ataques de BadUSB

Algunos virus modifican el firmware de los dispositivos USB para engañar al sistema operativo y que detecte el dispositivo USB y lo identifique como teclado.

El componente Prevención de ataques de BadUSB impide que dispositivos USB infectados que emulan un teclado se conecten al equipo.

Cuando un Dispositivo USB está conectado al equipo e identificado por la aplicación como un teclado, la aplicación solicita al usuario que introduzca un código numérico generado por la aplicación desde este teclado, o bien que utilice el teclado en pantalla (si está disponible). Este procedimiento se conoce como autorización del teclado. La aplicación permite el uso de un teclado autorizado y bloquea los teclados que no se hayan autorizado.

La Prevención de ataques de BadUSB se ejecuta en segundo plano en cuanto se instala el componente. Si la aplicación no está sujeta a una directiva de Kaspersky Security Center, puede activar o desactivar la Prevención de ataques de BadUSB [haciendo una pausa temporal y reanudando la protección y el control del equipo](#).

Instalación del componente Prevención de ataques de BadUSB

Si seleccionó la [instalación básica o estándar](#) durante la instalación de Kaspersky Endpoint Security, el componente Prevención de ataques de BadUSB no estará disponible. Para instalarlo, debe cambiar el conjunto de componentes de la aplicación.

Para instalar el componente Prevención de ataques de BadUSB:

1. En el menú **Inicio**, seleccione **Aplicaciones** → **Kaspersky Endpoint Security 10 para Windows** → **Modificar, reparar o quitar**.

Se iniciará el Asistente de instalación.

2. En la ventana **Modificar, reparar o eliminar aplicación** del Asistente de instalación de la aplicación, haga clic en el botón **Modificar**.

Esto abre la ventana **Instalación personalizada** del Asistente de instalación de la aplicación.

3. En el menú contextual del icono situado junto al nombre del componente **Prevención de ataques de BadUSB**, seleccione la opción **Esta función se instalará en el disco duro local**.

4. Haga clic en **Siguiente**.

5. Siga las instrucciones del Asistente de instalación.

Activación y desactivación de Prevención de ataques de BadUSB

Para activar o desactivar Prevención de ataques de BadUSB:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la sección **Prevención de ataques de BadUSB**.

La configuración de Prevención de ataques de BadUSB se muestra en la parte derecha de la ventana.

3. Realice una de las siguientes acciones:

- Para activar Prevención de ataques de BadUSB, seleccione la casilla de verificación **Activar Prevención de ataques de BadUSB**.
- Para desactivar Prevención de ataques de BadUSB, anule la selección de la casilla de verificación **Activar Prevención de ataques de BadUSB**.

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Permiso y prohibición de uso del teclado en pantalla para la autorización

El teclado en pantalla solo se debe utilizar para autorizar dispositivos USB que no permitan introducir caracteres aleatorios (p.ej., escáneres de códigos de barras). No se recomienda usar el teclado en pantalla para la autorización de dispositivos USB desconocidos.

Para permitir o prohibir el uso del teclado en pantalla para la autorización:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Protección antivirus**, seleccione la sección **Prevención de ataques de BadUSB**.

La configuración del componente se muestra en la parte derecha de la ventana.

3. Realice una de las siguientes acciones:

- Seleccione la casilla de verificación **Prohibir el uso del teclado en pantalla para la autorización** a fin de bloquear el uso del teclado en pantalla para la autorización.
- Borre la casilla de verificación **Prohibir el uso del teclado en pantalla para la autorización** a fin de permitir el uso del teclado en pantalla para la autorización.

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Autorización del teclado

Los dispositivos USB que identifique el sistema operativo como teclados y que se conecten al equipo antes de instalar el componente Prevención de ataques de BadUSB se considerarán autorizados después de la instalación del componente.

La aplicación requerirá que se autorice el dispositivo USB conectado que haya identificado el sistema operativo como teclado solo si está activada la solicitud de autorización del teclado USB. El usuario no podrá usar un teclado no autorizado hasta que se autorice.

Si se desactiva la solicitud de autorización del teclado USB, el usuario podrá usar todos los teclados conectados. Inmediatamente después de que se active la solicitud para autorizar el teclado USB, la aplicación muestra una solicitud de autorización para cada teclado no autorizado que esté relacionado.

Para autorizar un teclado:

1. Habiendo activado antes la autorización de teclado USB, conecte el teclado a un puerto USB.

La autorización del teclado **<Nombre del teclado>** se abre con los detalles del teclado conectado y un código numérico para su autorización.

2. Introduzca el código numérico generado al azar en la ventana de autorización desde el teclado conectado o Teclado en pantalla (si está disponible).

3. Haga clic en **Aceptar**.

Si se ha introducido el código correctamente, la aplicación guarda los parámetros de identificación (los VID y PID del teclado y el número del puerto al cual se ha conectado) en la lista de teclados autorizados. No será necesario volver a realizar la autorización cuando se vuelva a conectar el teclado o después de que se reinicie el sistema operativo.

Si el teclado autorizado se conecta al equipo a través de un puerto USB diferente, la aplicación volverá a mostrar la solicitud de autorización.

Si se introduce el código numérico de forma incorrecta, la aplicación generará un nuevo código. Se permitirá realizar tres intentos para introducir el código numérico. Si el código numérico se introduce de forma incorrecta tres veces seguidas o la ventana **Autorización del teclado <nombre del teclado>** se cierra, la aplicación bloqueará el uso del teclado. Si se vuelve a conectar el teclado o se reinicia el sistema operativo, la aplicación solicitará al usuario que realice de nuevo el procedimiento de autorización del teclado.

Control de inicio de aplicaciones

Esta sección contiene información sobre Control de inicio de aplicaciones, además de instrucciones sobre cómo configurar los parámetros del componente.

Acerca de Control de inicio de aplicaciones

El componente Control de inicio de aplicaciones supervisa los intentos del usuario de iniciar aplicaciones y regula el inicio de aplicaciones por medio de las [reglas de Control de inicio de aplicaciones](#).

El modo seleccionado para el funcionamiento del componente se encarga de regular el inicio de aplicaciones cuyos ajustes no coincidan con cualquiera de las reglas de Control de inicio de aplicaciones. El [modo de lista negra](#) se selecciona de forma predeterminada. Este modo permite que todos los usuarios puedan iniciar todas las aplicaciones.

Todos los intentos del usuario de iniciar aplicaciones se registran en [informes](#).



Activación y desactivación de Control de inicio de aplicaciones


Aunque el componente Control de inicio de las aplicaciones está deshabilitado por defecto, puede habilitarlo de ser necesario.

Existen dos formas de activar o desactivar el componente:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

Para activar o desactivar Control de inicio de aplicaciones en la pestaña Protección y control de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Control de Endpoint**.
Se abre la sección **Control de Endpoint**.
4. Haga clic con el botón derecho para que aparezca el menú contextual de la línea con información sobre el componente Control de inicio de aplicaciones.
Se abre un menú para seleccionar acciones sobre los componentes.
5. Realice una de las siguientes acciones:
 - Para activar Control de inicio de aplicaciones, seleccione **Iniciar** en el menú.
El icono de estado del componente , que se muestra a la izquierda en la línea **Control de inicio de aplicaciones**, cambia al icono .
 - Para desactivar el componente Control de inicio de aplicaciones, seleccione **Detener** en el menú.

El icono de estado del componente , que se muestra a la izquierda en la línea **Control de inicio de aplicaciones**, cambia al icono .

Para activar o desactivar Control de inicio de aplicaciones desde la ventana de configuración de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de inicio de aplicaciones**.

En la parte derecha de la ventana se muestra la configuración del componente Control de inicio de aplicaciones.

3. Realice una de las siguientes acciones:
 - Para activar Control de inicio de aplicaciones, seleccione la casilla de verificación **Activar Control de inicio de aplicaciones**.
 - Para desactivar Control de inicio de aplicaciones, desactive la casilla de verificación **Activar Control de inicio de aplicaciones**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Limitaciones de funcionalidad de Control de inicio de aplicaciones

El funcionamiento del componente Control de inicio de aplicaciones queda limitado en los casos siguientes:

- Cuando se actualiza la versión de la aplicación, no se admite la importación de la configuración del componente Control de inicio de aplicaciones.

Para restaurar la funcionalidad del Control de inicio de aplicaciones, debe configurar de nuevo los ajustes del componente.

- Si no hay conexión con los servidores del KSN, Kaspersky Endpoint Security recibe la información sobre la reputación de las aplicaciones y sus módulos solo desde las bases de datos locales. Si las bases de datos locales no contienen información sobre la aplicación, la aplicación no se categorizará en un grupo de confianza.

La categorización de aplicaciones cuando existe una conexión con servidores de KSN se puede diferenciar de la categorización cuando no hay conexión con KSN.

- En la base de datos de Kaspersky Security Center, es posible almacenar información acerca de 150 000 archivos procesados. Una vez que se alcance este número de archivos, no se procesarán nuevos archivos. Para reanudar las operaciones de inventario, debe eliminar los archivos que se inventariaron anteriormente en la base de datos de Kaspersky Security Center desde el equipo en el cual se instaló Kaspersky Endpoint Security.
- El componente no controla el inicio de scripts a menos que el script se envíe al intérprete mediante la línea de comandos.

Si está permitido el inicio de un intérprete por parte de reglas de Control de inicio de aplicaciones, el componente no bloqueará un script iniciado por este intérprete.

- El componente no controla el inicio de scripts desde aquellos intérpretes no admitidos por Kaspersky Endpoint Security.

Kaspersky Endpoint Security admite los siguientes intérpretes:

- Java
- PowerShell

Se admiten los siguientes tipos de intérpretes:

- { cCmdLineParser::itCmd, _T("%ComSpec%") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\system32\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\system32\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\system32\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\system32\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\system32\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\system32\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\system32\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\system32\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\system32\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\system32\wwahost.exe") };
- { cCmdLineParser::itCmd, _T("%SystemRoot%\syswow64\cmd.exe") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\syswow64\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\syswow64\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\syswow64\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\syswow64\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\syswow64\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\syswow64\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\syswow64\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\syswow64\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\syswow64\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\syswow64\wwahost.exe") }.

Acerca de las reglas de Control de inicio de aplicaciones

Kaspersky Endpoint Security controla el inicio de las aplicaciones que hayan realizado los usuarios por medio de reglas. Una regla de Control de inicio de aplicaciones especifica las condiciones de activación y la acción realizada por Control de inicio de aplicaciones cuando se activa la regla (lo que permite o impide a los usuarios que inicien la aplicación).

Condiciones de activación de reglas

Una condición para activar la regla tiene la siguiente correspondencia: "tipo de condición - criterio de condición - valor de condición" (consulte la figura siguiente). En función de las condiciones de activación de reglas, Kaspersky Endpoint Security aplicará (o no) la regla en cuestión a una aplicación.

Regla de Control de inicio de aplicaciones

Nombre de la regla:

Descripción:

Condiciones de inclusión:

Criterio de la condición	Valor de la condición
--------------------------	-----------------------

+ Agregar Modificar Eliminar Convertir en exclusión

Condiciones de exclusión:

Criterio de la condición	Valor de la condición
--------------------------	-----------------------

+ Agregar Modificar Eliminar Convertir a condición de inclusión

Entidades de seguridad y sus derechos:

Entidad de seguridad	Autorizar	Denegar
Everyone	<input type="checkbox"/>	<input checked="" type="checkbox"/>

+ Agregar Eliminar

Denegar para otros usuarios
 Programas de actualización de confianza

Ayuda Aceptar Cancelar

Regla de Control de inicio de aplicaciones. Parámetros de condición de activación de reglas

Las reglas utilizan condiciones de exclusión e inclusión:

- *Condiciones de inclusión.* Kaspersky Endpoint Security aplicará la regla a la aplicación si la aplicación cumple al menos una de las condiciones de inclusión.
- *Condiciones de exclusión.* Kaspersky Endpoint Security no aplicará la regla a la aplicación si la aplicación cumple al menos una de las condiciones de exclusión, pero no cumple ninguna de las condiciones de inclusión.

Las condiciones de activación de reglas se crean a partir de criterios. Los siguientes criterios se utilizan para crear reglas en Kaspersky Endpoint Security:

- Ruta de la carpeta que contiene el archivo ejecutable de la aplicación, o bien ruta al archivo ejecutable de la aplicación.

- Metadatos: nombre del archivo ejecutable de la aplicación, versión del archivo ejecutable de la aplicación, nombre de la aplicación, versión de la aplicación, proveedor de la aplicación.
- Hash del archivo ejecutable de la aplicación.
- Certificado: emisor, principal, huella digital.
- Inclusión de la aplicación en una categoría KL.
- Ubicación del archivo ejecutable de la aplicación en una unidad extraíble.

El valor del criterio se debe especificar para cada criterio utilizado en la condición. Si los parámetros de la aplicación que se va a iniciar coinciden con los valores de los criterios especificados en la condición de inclusión, la regla se activa. En este caso, Control de inicio de aplicaciones realiza la acción prescrita en la regla. Si los parámetros de la aplicación coinciden con los valores de los criterios especificados en la condición de exclusión, Control de inicio de aplicaciones no controla el inicio de la aplicación.

Decisiones tomadas por el componente Control de inicio de aplicaciones cuando se activa una regla

Cuando se activa una regla, Control de inicio de aplicaciones permitirá que los usuarios (o los grupos de usuarios) puedan iniciar aplicaciones o bloqueará el inicio de dichas aplicaciones, según lo que dicte la regla. Puede seleccionar usuarios particulares o grupos de usuarios que tienen o no permiso para iniciar aplicaciones que activan una regla.

A la regla que no especifica los usuarios que pueden iniciar aplicaciones que cumplan con la regla, se la denomina *regla de bloqueo*.

A la regla que no especifica los usuarios que no pueden iniciar aplicaciones que coincidan con la regla, se la denomina *regla de permiso*.

La prioridad de una regla de bloqueo es superior a la prioridad de una regla de permiso. Por ejemplo, si se ha especificado una regla de permiso de Control de inicio de aplicaciones para un grupo de usuarios y, al mismo tiempo, se ha especificado una regla de bloqueo de Control de inicio de aplicaciones para un usuario en este grupo de usuarios, se bloqueará a este usuario para que no ejecute la aplicación.

Estado operativo de una regla

Las reglas de Control de inicio de aplicaciones pueden tener uno de los dos valores de estado de funcionamiento:

- **Activo.**
Este estado de regla de funcionamiento indica que la regla está activada.
- **Inactivo.**
Este estado de regla indica que la regla está desactivada.

Reglas de Control de inicio de aplicaciones predeterminadas

De forma predeterminada, Control de inicio de aplicaciones funciona en el modo de lista negra. Este componente permite que todos los usuarios puedan iniciar todas las aplicaciones. Cuando un usuario intenta iniciar una aplicación bloqueada por las reglas de Control de inicio de aplicaciones, Kaspersky Endpoint Security bloquea el inicio de dicha aplicación (si se ha seleccionado la acción **Bloquear**) o guarda la información sobre el inicio de la aplicación en un informe (si se ha seleccionado la acción **Notificar**).

Gestión de reglas de Control de inicio de aplicaciones

Puede realizar las siguientes acciones para las reglas de Control de inicio de aplicaciones:

- Agregar una nueva regla.
- Crear o cambiar las condiciones para la activación de una regla
- Modificar el estado de la regla

Una regla de Control de inicio de aplicaciones puede estar activada (la casilla de verificación que hay junto a la regla está marcada) o desactivada (la casilla de verificación situada junto a la regla no se ha marcado). Una regla de Control de inicio de aplicaciones se activa de forma predeterminada después de crearse.

- Eliminar regla

Adición y edición de una regla de Control de inicio de aplicaciones

Para agregar o editar una regla de Control de inicio de aplicaciones:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de inicio de aplicaciones**.
En la parte derecha de la ventana se muestra la configuración del componente Control de inicio de aplicaciones.
3. Seleccione **Activar Control de inicio de aplicaciones** para permitir que la configuración del componente se pueda modificar.
4. Realice una de las siguientes acciones:
 - Para agregar una regla, haga clic en el botón **Agregar**.
 - Si desea modificar una regla existente, selecciónela en la lista de reglas y haga clic en el botón **Modificar**.

Se abre la ventana **Regla de Control de inicio de aplicaciones**.

5. Especifique o edite la configuración de la regla:
 - a. En el campo **Nombre de la regla**, introduzca o edite el nombre de la regla.
 - b. En la tabla **Condiciones de inclusión**, [cree](#) o edite la lista de condiciones de inclusión que activan una regla haciendo clic en los botones **Agregar**, **Editar**, **Eliminar** y **Convertir en exclusión**.

c. En la tabla **Condiciones de exclusión**, cree o edite la lista de condiciones de exclusión que activan una regla haciendo clic en los botones **Agregar**, **Editar**, **Eliminar** y **Convertir a condición de inclusión**.

d. Si es preciso, cambie el tipo de condición de activación de reglas:

- Para cambiar el tipo de condición de una condición de inclusión a una condición de exclusión, seleccione una condición en la tabla **Condiciones de inclusión** y haga clic en el botón **Convertir en exclusión**.
- Para cambiar el tipo de condición de una condición de exclusión a una condición de inclusión, seleccione una condición en la tabla **Condiciones de exclusión** y haga clic en el botón **Convertir a condición de inclusión**.

e. Recopile o edite una lista de usuarios y grupos de usuarios que tengan o no autorización para iniciar aplicaciones que cumplan las condiciones de activación de la regla. Para ello, haga clic en el botón **Agregar** en la tabla **Entidades de seguridad y sus derechos**.

Se abre la ventana **Seleccionar usuarios o grupos** en Microsoft Windows. Esta ventana le permite seleccionar usuarios o grupos de usuarios.

De forma predeterminada, el valor **Todos** se agrega a la lista de usuarios. La regla se aplica a todos los usuarios.

Si no hay ningún usuario especificado en la tabla, la regla no se puede guardar.

f. En la tabla **Entidades de seguridad y sus derechos**, seleccione las casillas de verificación **Permitir** o **Bloquear** situadas junto a los usuarios y los grupos de usuarios para determinar su derecho a iniciar aplicaciones.

La casilla de verificación que se selecciona de forma predeterminada depende del [modo de funcionamiento de Control de inicio de aplicaciones](#).

g. Seleccione la casilla de verificación **Denegar para otros usuarios** si desea evitar que los usuarios que no aparecen en la columna **Entidad de seguridad** y no forman parte del grupo de usuarios especificado en la columna **Entidad de seguridad** inicien aplicaciones que coincidan con las condiciones de activación de la regla.

Si la casilla de verificación **Denegar para otros usuarios** se desactiva, Kaspersky Endpoint Security no controla el inicio de aplicaciones por parte de usuarios no especificados en la tabla **Entidades de seguridad y sus derechos** y que no pertenecen a los grupos de usuarios especificados en dicha tabla **Entidades de seguridad y sus derechos**.

h. Si desea que Kaspersky Endpoint Security considere las aplicaciones que coinciden con las condiciones de activación de la regla como programas de actualización de confianza autorizados a iniciar otras aplicaciones para las que no se han definido reglas de Control de inicio de aplicaciones, seleccione la casilla de verificación **Programas de actualización de confianza**.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Adición de una condición de activación para una regla de Control de inicio de aplicaciones

Para añadir una nueva condición de activación para una regla de Control de inicio de aplicaciones:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de inicio de aplicaciones**.
En la parte derecha de la ventana se muestra la configuración del componente Control de inicio de aplicaciones.
3. Seleccione **Activar Control de inicio de aplicaciones** para permitir que la configuración del componente se pueda modificar.
4. Realice una de las siguientes acciones:
 - Si desea crear una nueva regla y agregar una condición de activación a dicha regla, haga clic en el botón **Agregar**.
 - Si desea agregar una condición de activación a una regla existente, seleccione la regla en la lista de reglas y haga clic en el botón **Editar**.

Se abre la ventana **Regla de Control de inicio de aplicaciones**.

5. En la tabla **Condiciones de inclusión** o tabla **Condiciones de exclusión**, haga clic en el botón **Agregar**.

Puede usar la lista desplegable del botón **Agregar** para agregar varias condiciones de activación a la regla (consulte las instrucciones a continuación).

Para añadir una condición de activación de reglas en función de las propiedades de los archivos de una carpeta específica:

1. En la lista desplegable del botón **Agregar**, seleccione **Condición(es) de las propiedades de los archivos en la carpeta especificada**.
Se abre la ventana estándar **Seleccionar carpeta** de Microsoft Windows.
2. En la ventana **Seleccionar carpeta**, seleccione una carpeta que contenga los archivos ejecutables de las aplicaciones cuyas propiedades desee utilizar como base para una o varias condiciones de activación de una regla.
3. Haga clic en **Aceptar**.
Se abre la ventana **Agregar condición**.
4. En la lista desplegable **Mostrar criterio**, seleccione el criterio basado en el cual desea crear una o varias condiciones de activación de la regla: **Código hash del archivo**, **Certificado**, **Categoría KL**, **Metadatos** o **Ruta de la carpeta**.

Kaspersky Endpoint Security no admite código hash de un archivo MD5 y no controla el inicio de aplicaciones basado en un hash de MD5. Se utiliza un hash SHA256 como condición de activación de reglas.

5. Si seleccionó **Metadatos** en la lista desplegable **Mostrar criterio**, seleccione las casillas de verificación situadas junto a las propiedades del archivo ejecutable que desee utilizar en la condición de activación de la regla: **Nombre del archivo**, **Versión del archivo**, **Nombre de aplicación**, **Versión de la aplicación** y **Proveedor**.
Si no se selecciona ninguna de las propiedades especificadas, la regla no se puede guardar.

6. Si seleccionó **Certificado** en la lista desplegable **Mostrar criterio**, seleccione las casillas de verificación situadas junto a la configuración que desea usar en la condición de activación de reglas **Emisor**, **Principal** y **Huella digital**.

Si no se selecciona ninguno de los ajustes especificados, la regla no se puede guardar.

No se recomienda utilizar únicamente los criterios **Emisor** y **Entidad de seguridad** como condiciones de activación de la regla. El uso de estos criterios no es fiable.

7. Seleccione las casillas de verificación que hay junto a los nombres de los archivos ejecutables de la aplicación cuyas propiedades desee incluir en las condiciones de activación de la regla.
8. Haga clic en **Siguiente**.
Aparece una lista de condiciones de activación de reglas formuladas.
9. En la lista de condiciones de activación de reglas formuladas, seleccione las casillas de verificación que hay junto a las condiciones de activación de reglas que desee agregar a la regla de Control de inicio de aplicaciones.
10. Haga clic en el botón **Terminar**.

Para agregar una condición de activación de reglas en función de las propiedades de las aplicaciones que se iniciaron en el equipo:

1. En la lista desplegable del botón **Agregar**, seleccione **Condición(es) de propiedades de las aplicaciones iniciadas**.
2. En la ventana **Agregar condición** (en la lista desplegable **Mostrar criterio**), seleccione el criterio en función del cual quiera crear una o varias condiciones de activación de la regla: **Código hash de archivo**, **Certificado**, **Categoría KL**, **Metadatos** o **Ruta de acceso a carpeta**.
3. Si seleccionó **Metadatos** en la lista desplegable **Mostrar criterio**, seleccione las casillas de verificación situadas junto a las propiedades del archivo ejecutable que desee utilizar en la condición de activación de la regla: **Nombre del archivo**, **Versión del archivo**, **Nombre de aplicación**, **Versión de la aplicación** y **Proveedor**.
Si no se selecciona ninguna de las propiedades especificadas, la regla no se puede guardar.
4. Si seleccionó **Certificado** en la lista desplegable **Mostrar criterio**, seleccione las casillas de verificación situadas junto a la configuración que desea usar en la condición de activación de reglas: **Emisor**, **Entidad de seguridad** y **Huella digital**.

Si no se selecciona ninguno de los ajustes especificados, la regla no se puede guardar.

No se recomienda utilizar únicamente los criterios **Emisor** y **Entidad de seguridad** como condiciones de activación de la regla. El uso de estos criterios no es fiable.

5. Seleccione las casillas de verificación que hay junto a los nombres de los archivos ejecutables de la aplicación cuyas propiedades desee incluir en las condiciones de activación de la regla.
6. Haga clic en **Siguiente**.
Aparece una lista de condiciones de activación de reglas formuladas.
7. En la lista de condiciones de activación de reglas formuladas, seleccione las casillas de verificación que hay junto a las condiciones de activación de reglas que desee agregar a la regla de Control de inicio de aplicaciones.
8. Haga clic en el botón **Terminar**.

Para añadir una condición de activación de reglas basada en la categoría KL:

1. En la lista desplegable del botón **Agregar**, seleccione **Condición(es) "Categoría KL"**.

Una *categoría KL* es una lista de aplicaciones que han compartido atributos de tema. Los expertos de Kaspersky se encargan del mantenimiento de la lista. Por ejemplo, la categoría KL de "Aplicaciones de Office" incluye todas las aplicaciones del paquete Microsoft Office y Adobe® Acrobat®, entre otros.

2. En la ventana **Condición(es) "Categoría KL"**, seleccione las casillas situadas junto a los nombres de las categorías KL en función de las cuales desea crear condiciones de activación de reglas.
3. Haga clic en **Aceptar**.

Para agregar una condición de activación de reglas personalizada:

1. En la lista desplegable del botón **Agregar**, seleccione **Condición de las propiedades del archivo**.
2. En la ventana **Condición personalizada**, haga clic en el botón **Seleccionar** y especifique la ruta al archivo ejecutable de la aplicación.
3. Seleccione el criterio según que desea crear una condición de activación de reglas: **Código hash del archivo**, **Certificado**, **Metadatos** o **Ruta al archivo o carpeta**.

Si está usando enlaces simbólicos en el campo **Ruta al archivo o carpeta**, le aconsejamos resolver los enlaces simbólicos para que la regla de Control de Inicio de Aplicaciones funcione correctamente. Para ello, haga clic en el botón **Resolver enlace simbólico**.

4. Si es necesario, configure los ajustes del criterio seleccionado.
5. Haga clic en **Aceptar**.

Para añadir una condición de activación de reglas basada en la información de la unidad que almacena el archivo ejecutable de una aplicación:

1. En la lista desplegable del botón **Agregar**, seleccione **Condición por unidad de archivos**.
2. En la ventana **Condición por unidad de archivos**, en la lista desplegable **Unidad**, seleccione el tipo de unidad desde la que el inicio de aplicaciones servirá como condición de activación de reglas.
3. Haga clic en **Aceptar**.

Cambiar el estado de una regla de Control de inicio de aplicaciones

Para cambiar el estado de una regla de Control de inicio de aplicaciones:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de inicio de aplicaciones**.

En la parte derecha de la ventana se muestra la configuración del componente Control de inicio de aplicaciones.

3. Seleccione **Activar Control de inicio de aplicaciones** para permitir que la configuración del componente se pueda modificar.
4. Seleccione la regla cuyo estado quiera editar.
5. En la columna **Estado**, haga lo siguiente:
 - Si desea activar el uso de una regla, seleccione la casilla de verificación que hay junto a la regla.
 - Si desea desactivar el uso de una regla, desactive la casilla de verificación que hay junto a la regla.
6. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Probar reglas de Control de inicio de aplicaciones

Para asegurarse de que las reglas de Control de inicio de aplicaciones no bloquean las aplicaciones requeridas para el trabajo, se recomienda poner a prueba las reglas de creación reciente y analizar su funcionamiento.

Un análisis del funcionamiento de las reglas de Control de inicio de aplicaciones requiere la revisión de los eventos de Control de inicio de aplicaciones que se notifican a Kaspersky Security Center. Si se permite que se inicien todas las aplicaciones requeridas para el trabajo del usuario del equipo, las reglas se han creado correctamente. Si no, recomendamos que revise la configuración de las reglas que creó.

El modo de prueba para las reglas de Control de inicio de aplicaciones se desactiva de forma predeterminada.

Para probar las reglas de Control de inicio de aplicaciones:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de inicio de aplicaciones**.
En la parte derecha de la ventana se muestra la configuración del componente Control de inicio de aplicaciones.
3. Seleccione **Activar Control de inicio de aplicaciones** para permitir que la configuración del componente se pueda modificar.
4. En la lista desplegable **Regla de Control de inicio de aplicaciones**, seleccione uno de los elementos siguientes:
 - **Lista negra**, si desea permitir el inicio de todas las aplicaciones excepto las especificadas en reglas de bloqueo.
 - **Lista blanca**, si desea bloquear el inicio de todas las aplicaciones excepto las especificadas en reglas de autorización.
5. En la lista desplegable **Acción**, seleccione **Notificar**.
6. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Kaspersky Endpoint Security no bloqueará las aplicaciones cuyo inicio está prohibido por las reglas de Control de inicio de aplicaciones, pero enviará notificaciones sobre su inicio al servidor de administración.

Edición de plantillas de mensajes de Control de inicio de aplicaciones

Cuando un usuario intenta iniciar una aplicación que se encuentra bloqueada por una regla de Control de inicio de aplicaciones, Kaspersky Endpoint Security muestra un mensaje que indica que la aplicación está bloqueada desde el inicio. Si el usuario cree que el inicio de la aplicación se bloqueó por error, puede utilizar el enlace del texto del mensaje para enviar un mensaje al administrador de la red de área local.

Existen plantillas especiales disponibles para el mensaje que se muestra cuando se bloquea el inicio de una aplicación y para el mensaje que se envía al administrador. Puede modificar las plantillas de los mensajes.

Para editar una plantilla de mensaje:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de inicio de aplicaciones**.
En la parte derecha de la ventana se muestra la configuración del componente Control de inicio de aplicaciones.
3. Seleccione **Activar Control de inicio de aplicaciones** para permitir que la configuración del componente se pueda modificar.
4. Haga clic en el botón **Plantillas**.
Se abre la ventana **Plantillas de mensajes**.
5. Realice una de las siguientes acciones:
 - Si desea editar la plantilla del mensaje que se muestra cuando el inicio de una aplicación está bloqueado, seleccione la pestaña **Bloqueo**.
 - Si desea modificar la plantilla del mensaje que se envía al administrador de la LAN, seleccione la pestaña **Mensaje al administrador**.
6. Modifique la plantilla del mensaje que se muestra cuando se bloquea el inicio de una aplicación o el mensaje se envía al administrador. Para ello, utilice los botones **Predeterminado** y **Variable**.
7. Haga clic en **Aceptar**.
8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Acerca de los modos de funcionamiento de Control de inicio de aplicaciones

El componente Control de inicio de aplicaciones funciona en dos modos:

- **Lista negra.** En este modo, Control de inicio de aplicaciones autoriza a todos los usuarios a que inicien todas las aplicaciones, excepto aquellas que se especifican en las [reglas de bloqueo de Control de inicio de aplicaciones](#). Este modo del componente Control de inicio de aplicaciones está activado de forma predeterminada.
- **Lista blanca.** En este modo, el componente Control de inicio de aplicaciones bloquea a todos los usuarios para evitar que inicien cualquier aplicación, excepto aquellas que se especifican en las reglas de autorización de

Control de inicio de aplicaciones.

Si las reglas de autorización de Control de inicio de aplicaciones están totalmente configuradas, el componente bloquea el inicio de todas las aplicaciones nuevas que no haya verificado el administrador de la red de área local desde su inicio, mientras que autoriza el funcionamiento del sistema operativo y de las aplicaciones de confianza en las que los usuarios confían en su trabajo.

Cada modo tiene dos acciones que se pueden llevar a cabo en aplicaciones en ejecución: Kaspersky Endpoint Security puede bloquear el inicio de las aplicaciones o notificar al usuario sobre el inicio de una aplicación que coincida con las condiciones de las reglas de Control de inicio de aplicaciones.

El Control de inicio de aplicaciones puede configurarse para que funcione en estos modos tanto mediante la interfaz local de Kaspersky Endpoint Security como mediante Kaspersky Security Center.

Sin embargo, Kaspersky Security Center ofrece herramientas que no están disponibles en la interfaz local de Kaspersky Endpoint Security, como las herramientas que son necesarias para las siguientes tareas:

- [Creación de categorías de aplicaciones.](#)

Las reglas del componente Control de inicio de aplicaciones de la consola de administración de Kaspersky Security Center se basan en categorías de aplicaciones predeterminadas, y no en reglas de inclusión y exclusión, como sucede en la interfaz local de Kaspersky Endpoint Security.

- [Recopilación de información acerca de las aplicaciones que están instaladas en los equipos de la LAN.](#)

Por esto, se recomienda usar Kaspersky Security Center para configurar el funcionamiento del componente Control de inicio de aplicaciones.

Seleccionar el modo de Control de inicio de aplicaciones

Para seleccionar el modo de Control de inicio de aplicaciones:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de inicio de aplicaciones**.

En la parte derecha de la ventana se muestra la configuración del componente Control de inicio de aplicaciones.

3. Seleccione **Activar Control de inicio de aplicaciones** para permitir que la configuración del componente se pueda modificar.

4. En la lista desplegable **Regla de Control de inicio de aplicaciones**, seleccione una de las opciones siguientes:

- **Lista negra**, si desea permitir el inicio de todas las aplicaciones excepto las especificadas en reglas de bloqueo.
- **Lista blanca**, si desea bloquear el inicio de todas las aplicaciones excepto las especificadas en reglas de autorización.

Cuando este modo se selecciona, se crean dos reglas de Control de inicio de aplicaciones de forma predeterminada: **Golden Image** y **Programas de actualización de confianza**. No puede eliminar estas reglas. La configuración de estas reglas no se puede editar. Puede activar o desactivar estas reglas al seleccionar o al desactivar la casilla situada junto a la regla pertinente. De forma predeterminada, la regla **Golden Image** está activada y la regla **Programas de actualización de confianza** está desactivada. Todos los usuarios tienen permiso para iniciar aplicaciones que cumplan las condiciones de activación de estas reglas.

Todas las reglas creadas durante el modo seleccionado se guardan después de cambiar el modo, de manera que las reglas se pueden utilizar de nuevo. Para volver a utilizar estas reglas, solo tiene que seleccionar el modo necesario en la lista desplegable **Regla de Control de inicio de aplicaciones**.

5. En la lista desplegable **Acción**, seleccione la acción que realizará el componente cuando un usuario intente iniciar una aplicación bloqueada por reglas de Control de inicio de aplicaciones.
6. Seleccione **Supervisar DLL y los controladores** si desea que Kaspersky Endpoint Security supervise la carga de módulos DLL cuando los usuarios inician aplicaciones.

La información sobre el módulo y la aplicación que cargó dicho módulo se guardará en un informe.

Si la casilla de verificación está seleccionada, los módulos DLL y controladores se supervisan antes de que se inicie Kaspersky Endpoint Security. Para configurar la supervisión posterior de todos los módulos DLL y controladores antes del inicio de la aplicación, reinicie el equipo después de seleccionar la casilla de verificación **Supervisar DLL y los controladores**. Si no puede reiniciar el equipo, después de seleccionar la casilla de verificación **Supervisar DLL y los controladores**, puede cargar módulos DLL y controladores mientras se ejecuta Kaspersky Endpoint Security. En este caso, la supervisión solo se realiza para los módulos de DLL y controladores que se cargan mientras se ejecuta Kaspersky Endpoint Security.

Al supervisar módulos de DLL y controladores, no se recomienda usar reglas de Control de Inicio de Aplicaciones que se crearon a partir de categorías KL. Es posible que la determinación de categorías KL (incluidas en las reglas "Sistema operativo y sus componentes") para módulos DLL y controladores no funcione correctamente. En particular, la regla "Sistema operativo y sus componentes" se creó de forma predeterminada y no se distribuye al iniciar los módulos DLL y controladores. Al activar esta función, es necesario crear reglas de autorización separadas para módulos DLL y controladores. Si tal regla de autorización no existe, el uso de la función **Control de DLL y controladores** podría volver inestable el sistema.

Recomendamos activar la protección con contraseña para configurar los ajustes del programa, de modo que sea posible desactivar las reglas de autorización que bloquean el inicio de módulos DLL y controladores importantes sin cambiar la configuración de la directiva de Kaspersky Security Center en el proceso.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Gestionar reglas de Control de inicio de aplicaciones con Kaspersky Security Center

Esta sección contiene información sobre la utilización de Kaspersky Security Center para configurar reglas de Control de inicio de aplicaciones y proporciona recomendaciones sobre el uso óptimo de Control de inicio de aplicaciones.

Recopilación de información acerca de las aplicaciones instaladas en los equipos de los usuarios

Para crear reglas óptimas de Control de inicio de aplicaciones, se recomienda obtener primero una imagen de las aplicaciones que se utilizan en los equipos de la red de área local. Para ello, puede obtener la siguiente información:

- Proveedores, versiones y localizaciones de las aplicaciones utilizadas en la red de área local corporativa.
- Frecuencia de las actualizaciones de la aplicación.
- Las directivas de uso de aplicaciones adoptadas en la empresa (puede tratarse de directivas de seguridad o directivas administrativas).
- Ubicación donde se almacenan los paquetes de distribución de la aplicación.

La información acerca de las aplicaciones que se utilizan en los equipos de la red de área local corporativa está disponible en las carpetas **Registro de aplicaciones** y **Archivos ejecutables**. Las carpetas **Registro de aplicaciones** y **Archivos ejecutables** están ubicadas en la carpeta **Gestión de aplicaciones** del árbol de la consola de administración de Kaspersky Security Center.

La carpeta **Registro de aplicaciones** contiene la lista de aplicaciones que detectó el [Agente de red](#) instalado en el equipo cliente.

La carpeta **Archivos ejecutables** contiene una lista de los archivos ejecutables que se han iniciado en los equipos cliente o se han detectado durante la [tarea de inventario de Kaspersky Endpoint Security](#).

Para ver la información general acerca de la aplicación y sus archivos ejecutables, así como la lista de equipos en los que se instala una aplicación, abra la ventana de propiedades de una aplicación que esté seleccionada en la carpeta **Registro de aplicaciones** o en la carpeta **Archivos ejecutables**.

Creación de categorías de aplicaciones

Para que crear reglas resulte más práctico, puede crear categorías de aplicaciones y utilizarlas al crear reglas de Control de inicio de aplicaciones.

Se recomienda crear una categoría "Aplicaciones de trabajo" que abarque el conjunto estándar de las aplicaciones que se utilicen en la empresa. Si hay distintos grupos de usuarios que utilicen distintos conjuntos de aplicaciones en su trabajo, puede crearse una categoría de aplicaciones independiente para cada grupo de usuarios.

Para crear una categoría de aplicaciones:

1. Abra la consola de administración de Kaspersky Security Center.
2. En el árbol de la consola de administración, seleccione la carpeta **Avanzado** → **Gestión de aplicaciones** → **Categorías de aplicaciones**.
3. Haga clic en el botón **Crear categoría** en el espacio de trabajo.
Se iniciará el asistente de creación de categorías del usuario.
4. Siga las instrucciones de dicho asistente de creación de categorías.

Crear reglas de Control de inicio de aplicaciones con Kaspersky Security Center

Para crear una regla de Control de inicio de aplicaciones con Kaspersky Security Center:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Control de Endpoint**, seleccione el apartado **Control de inicio de aplicaciones**.
En la parte derecha de la ventana se muestra la configuración del componente Control de inicio de aplicaciones.
7. Haga clic en el botón **Agregar**.
Se abre la ventana **Regla de Control de inicio de aplicaciones**.
8. En la lista desplegable **Categoría**, seleccione la categoría de aplicación en función de la cual desea crear una regla.
9. Especifique la lista de usuarios y grupos de usuarios para los que desea configurar los permisos para iniciar aplicaciones de la categoría seleccionada. Para ello, en la tabla **Entidades de seguridad y sus derechos**, haga clic en el botón **Agregar**.
Se abre la ventana estándar **Seleccionar usuarios o grupos** en Microsoft Windows. Esta ventana le permite seleccionar usuarios o grupos de usuarios.
10. En la tabla **Entidades de seguridad y sus derechos**:
 - Si desea permitir que los usuarios y los grupos de usuarios inicien aplicaciones que pertenecen a la categoría seleccionada, seleccione las casillas de verificación **Permitir** situadas junto a esos usuarios.
 - Si desea bloquear a usuarios y grupos de usuarios desde aplicaciones que se inician y pertenecen a la categoría seleccionada, seleccione la casilla de verificación **Bloquear** situada junto a esos usuarios.
11. Seleccione la casilla de verificación **Rechazar para otros usuarios** si desea que se bloquee la posibilidad todos los usuarios que no aparezcan en la columna **Entidad de seguridad** y que no forman parte del grupo de usuarios especificados en la columna **Entidad de seguridad** inicien aplicaciones.
12. Si desea que Kaspersky Endpoint Security considere las aplicaciones de la categoría especificada en la regla como programas de actualización de confianza, y que tengan permiso para iniciar otras aplicaciones para las que no se hayan definido reglas de Control de inicio de aplicaciones, seleccione la casilla de verificación **Programas de actualización de confianza**.

13. Haga clic en **Aceptar**.

14. En la sección **Control de inicio de aplicaciones** de la ventana de propiedades de la directiva, haga clic en el botón **Aplicar**.

Cambio del estado de una regla de Control de inicio de aplicaciones mediante Kaspersky Security Center

Para cambiar el estado de una regla de Control de inicio de aplicaciones:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Control de Endpoint**, seleccione el apartado **Control de inicio de aplicaciones**.
En la parte derecha de la ventana se muestra la configuración del componente Control de inicio de aplicaciones.
7. Seleccione la regla de Control de inicio de aplicaciones cuyo estado desee cambiar.
8. En la columna **Estado**, lleve a cabo una de las siguientes acciones:
 - Si desea activar el uso de una regla, seleccione la casilla de verificación que hay junto a la regla.
 - Si desea desactivar el uso de una regla, desactive la casilla de verificación que hay junto a la regla.
9. Haga clic en el botón **Aplicar**.

Control de actividad de aplicaciones

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security se instala en un equipo con [Microsoft Windows para servidores de archivos](#).

Esta sección contiene información sobre Control de actividad de aplicaciones, además de instrucciones sobre cómo configurar los parámetros del componente.

Acerca de Control de actividad de aplicaciones

Control de actividad de aplicaciones evita que las aplicaciones realicen acciones que puedan resultar peligrosas para el sistema operativo; además, garantiza el control del acceso a los recursos del sistema operativo y a los datos de identidad.

Este componente controla la actividad de las aplicaciones, entre las que se incluyen el acceso a recursos protegidos (como archivos, carpetas, claves de registro), mediante el uso de *reglas de control de aplicaciones*. Las reglas de control de aplicaciones son un conjunto de restricciones que se aplican a varias acciones de aplicaciones del sistema operativo y a los derechos de acceso a los recursos del equipo.

El componente Firewall supervisa la actividad de red de las aplicaciones.

Cuando una aplicación se inicia por primera vez, Control de actividad de aplicaciones analiza la aplicación y la ubica en un grupo de confianza. Un grupo de confianza define las reglas de control de aplicaciones que Kaspersky Endpoint Security aplica cuando controla la actividad de las aplicaciones.

Le recomendamos que [participe en Kaspersky Security Network](#) para que el componente Control de actividad de aplicaciones sea más efectivo. Los datos que se obtienen a través de Kaspersky Security Network le permiten ordenar las aplicaciones en grupos con más precisión. Además, puede aplicar reglas de control de aplicaciones óptimas.

La próxima vez que se inicie la aplicación, Control de actividad de aplicaciones verificará la integridad de la aplicación. Si no se ha modificado la aplicación, el componente aplica las reglas de control de aplicaciones actuales. Si se ha modificado la aplicación, Control de actividad de aplicaciones vuelve a analizarla como si fuese la primera vez que se inicia.

Limitaciones del control de dispositivos de audio y de vídeo

Acerca de la protección del flujo de audio

La protección del flujo de audio tiene las siguientes consideraciones especiales:

- El componente Control de actividad de aplicaciones se debe activar para que esta funcionalidad esté activa.
- Si la aplicación empezó a recibir el flujo de audio antes de que se iniciara el componente Control de actividad de aplicaciones, Kaspersky Endpoint Security permite que la aplicación reciba el flujo de audio y no muestre

ninguna notificación.

- Si movió la aplicación al grupo **No confiable** o al grupo **Restricción máxima** después de que la aplicación comenzase a recibir el flujo de audio, Kaspersky Endpoint Security permite que la aplicación reciba el flujo de audio y no muestra ninguna notificación.
- Después de modificar la configuración del acceso de las aplicaciones a dispositivos de grabación de sonido (por ejemplo, si se ha bloqueado la recepción del flujo de audio por parte de la aplicación en la ventana de configuración de Control de aplicaciones), esta aplicación se debe reiniciar para que deje de recibir el flujo de audio.
- El control del acceso al flujo de audio desde dispositivos de grabación de sonido no depende de la configuración de acceso a la cámara web de una aplicación.
- Kaspersky Endpoint Security protege el acceso únicamente los micrófonos integrados y micrófonos externos. El resto de los dispositivos de flujo de audio no son compatibles.
- Kaspersky Endpoint Security no puede garantizar la protección de un flujo de audio desde dispositivos como cámaras DSLR, videocámaras portátiles y cámaras de acción.

Consideraciones especiales para el funcionamiento de los dispositivos de audio y de vídeo durante la instalación y la actualización de Kaspersky Endpoint Security

Al ejecutar aplicaciones de reproducción o grabación de audio y vídeo por primera vez desde la instalación de Kaspersky Endpoint Security, es posible que se interrumpa la reproducción o la grabación de audio y vídeo. Esto es necesario a fin de activar la funcionalidad que controla el acceso a los dispositivos de grabación de sonido por aplicaciones. El servicio del sistema que controla el hardware de audio se reiniciará cuando Kaspersky Endpoint Security se ejecute por primera vez.

Acerca del acceso a cámaras web por aplicaciones

La funcionalidad de protección del acceso a la cámara web tiene las siguientes consideraciones especiales y limitaciones:

- La aplicación controla el vídeo y las imágenes estáticas derivados del procesamiento de los datos de la cámara web.
- La aplicación controla el flujo de audio si este forma parte del flujo de vídeo recibido a través de la cámara web.
- La aplicación controla solo las cámaras web conectadas mediante USB o IEEE1394 que se muestran como **Dispositivos de imagen** en el Administrador del dispositivos de Windows.

Cámaras web admitidas

Kaspersky Endpoint Security admite las siguientes cámaras web:

- Cámara web Logitech HD C270
- Cámara web Logitech HD C310
- Cámara web Logitech C210
- Cámara web Logitech Pro 9000

- Cámara web Logitech HD C525
- Microsoft LifeCam VX-1000
- Microsoft LifeCam VX-2000
- Microsoft LifeCam VX-3000
- Microsoft LifeCam VX-800
- Microsoft LifeCam Cinema

Kaspersky no puede garantizar la compatibilidad con las cámaras web que no se especifican en esta lista.

Activación y desactivación de Control de actividad de aplicaciones

De forma predeterminada, Control de actividad de aplicaciones está activado y se ejecuta en un modo recomendado por los expertos de Kaspersky. Si fuera necesario, puede desactivar Control de actividad de aplicaciones.

Existen dos formas de activar o desactivar el componente:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

Para activar o desactivar Control de actividad de aplicaciones, haga lo siguiente en la pestaña Protección y control de la ventana principal de la aplicación:

1. Abra la ventana principal de la aplicación.

2. Seleccione la pestaña **Protección y control**.

3. Haga clic en la sección **Control de Endpoint**.



Se abre la sección **Control de Endpoint**.

4. Haga clic con el botón derecho para mostrar el menú contextual de la línea con información sobre el componente Control de actividad de aplicaciones.



Se abre un menú para seleccionar acciones sobre los componentes.

5. Realice una de las siguientes acciones:

- Para activar Control de actividad de aplicaciones, seleccione **Iniciar**.

El icono de estado del componente , que se muestra a la parte izquierda en la línea Control de actividad de aplicaciones, cambia al icono .

- Para desactivar el componente Control de actividad de aplicaciones, seleccione **Detener**.

El icono de estado del componente , que se muestra a la parte izquierda en la línea Control de actividad de aplicaciones, cambia al icono .

Para activar o desactivar Control de actividad de aplicaciones desde la ventana de configuración de la aplicación:

1. Abra la ventana de configuración de la aplicación.

2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de actividad de aplicaciones**.

En la parte derecha de la ventana, se muestra la configuración del componente Control de actividad de aplicaciones.

3. En la parte derecha de la ventana, seleccione una de las siguientes acciones:

- Para activar Control de actividad de aplicaciones, seleccione la casilla de verificación **Activar Control de actividad de aplicaciones**.
- Para desactivar Control de actividad de aplicaciones, desactive la casilla de verificación **Activar Control de actividad de aplicaciones**.

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Gestionar grupos de confianza de aplicaciones

Cuando la aplicación se inicia por primera vez, el componente Control de actividad de aplicaciones comprueba la seguridad de la aplicación y la coloca en un [grupo de confianza](#).

En la primera etapa del análisis de la aplicación, Kaspersky Endpoint Security busca una entrada coincidente en la base de datos interna de aplicaciones conocidas y, a continuación, envía una solicitud a la base de datos de [Kaspersky Security Network](#) (si se dispone de conexión a Internet). Según los resultados de la búsqueda en la base de datos interna y la base de datos de Kaspersky Security Network, la aplicación se sitúa en un grupo de confianza. Cada vez que la aplicación se inicia, Kaspersky Endpoint Security envía una nueva consulta a la base de datos de KSN y sitúa la aplicación en un grupo de confianza diferente si la reputación de la aplicación en las bases de datos de KSN ha cambiado.

Puede seleccionar un grupo de confianza al que Kaspersky Endpoint Security asigne automáticamente todas las aplicaciones desconocidas. Las aplicaciones que se iniciaron antes de Kaspersky Endpoint Security se mueven automáticamente al grupo de confianza especificado en la ventana [Seleccionar grupo de confianza](#).

El componente solo controla la actividad de red de las aplicaciones iniciadas antes de Kaspersky Endpoint Security según el conjunto de reglas de red de la configuración del Firewall.

Configurar los ajustes para asignar aplicaciones a grupos de confianza

Si se activa la participación en Kaspersky Security Network, Kaspersky Endpoint Security envía a KSN una consulta sobre la reputación de una aplicación cada vez que la aplicación se inicia. Según la respuesta de KSN, la aplicación se puede mover a un grupo de confianza distinto al especificado en la configuración de Control de Actividad de Aplicaciones.

Para configurar los valores para la ubicación de aplicaciones en grupos de confianza:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de actividad de aplicaciones**.

En la parte derecha de la ventana, se muestra la configuración del componente Control de actividad de aplicaciones.

3. Si desea ubicar automáticamente aplicaciones con firma digital de proveedores de confianza en el grupo de confianza, seleccione la casilla de verificación **Confiar en las aplicaciones que tengan una firma digital**.

Los proveedores de confianza son proveedores de software que figuran dentro del grupo de confianza de Kaspersky. También puede [añadir un certificado de proveedor al almacén de confianza de certificados del sistema de forma manual](#).

4. Seleccione la manera en la que las aplicaciones desconocidas se asignan a grupos de confianza:
 - Para utilizar el análisis heurístico con el fin de asignar aplicaciones desconocidas a grupos de confianza, seleccione la opción **Usar análisis heurístico para definir grupo** y especifique el periodo de tiempo asignado para analizar la aplicación iniciada en el campo **Tiempo máximo para definir el grupo**.
 - Si desea asignar todas las aplicaciones desconocidas a un grupo de confianza específico, seleccione la opción **Mover automáticamente a grupo** y seleccione el grupo de confianza apropiado en la lista desplegable.

Por razones de seguridad, el grupo **De confianza** no se incluye en los valores del ajuste **Mover automáticamente a grupo**.

5. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Modificación de un grupo de confianza

Cuando una aplicación se inicia por primera vez, Kaspersky Endpoint Security coloca dicha aplicación en un grupo de confianza automáticamente. Si es necesario, puede mover la aplicación a otro grupo de confianza manualmente.

Los especialistas de Kaspersky no recomiendan mover aplicaciones del grupo de confianza asignado automáticamente a otro grupo diferente. En lugar de eso, puede editar las reglas de una aplicación individual.

Para modificar el grupo de confianza al que Kaspersky Endpoint Security ha asignado automáticamente una aplicación cuando se ha iniciado por primera vez:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de actividad de aplicaciones**.

En la parte derecha de la ventana, se muestra la configuración del componente Control de actividad de aplicaciones.
3. Haga clic en el botón **Aplicaciones**.

Se abre la pestaña **Reglas de Control de aplicaciones** en la ventana **Aplicaciones**.
4. Seleccione la aplicación pertinente en la pestaña **Reglas de Control de aplicaciones**.
5. Realice una de las siguientes acciones:

- Haga clic con el botón derecho para que aparezca el menú contextual de la aplicación. En el menú contextual de la aplicación, seleccione **Mover al grupo** → <νομβρε δελ γρυπο>.
- Para abrir el menú contextual, haga clic en el enlace **De confianza / Restricción mínima / Restricción máxima / No confiable**. En el menú contextual, seleccione el grupo de confianza requerido.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Seleccionar un grupo de confianza para aplicaciones iniciadas antes que Kaspersky Endpoint Security

El componente solo controla la actividad de red de las aplicaciones que se iniciaron antes que Kaspersky Endpoint Security. El control se realiza según las reglas de red especificadas en [Configuración del Firewall](#). Para especificar qué reglas de red se deben aplicar a la supervisión de la actividad de la red de tales aplicaciones, debe seleccionar un grupo de confianza.

Para seleccionar el grupo de confianza de las aplicaciones iniciadas antes que Kaspersky Endpoint Security:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de actividad de aplicaciones**.
En la parte derecha de la ventana, se muestra la configuración del componente Control de actividad de aplicaciones.
3. Haga clic en el botón **Modificar**.
Este botón abre la ventana **Seleccionar grupo de confianza**.
4. Seleccione el grupo de confianza pertinente.
5. Haga clic en **Aceptar**.
6. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Gestión de reglas de Control de aplicaciones

De forma predeterminada, las reglas de control de aplicaciones, que se definen para el grupo de confianza al que Kaspersky Endpoint Security asignó la aplicación cuando se inició por primera vez, son las que controlan la actividad de la aplicación. Si es necesario, puede editar las reglas de control de aplicaciones para todo un grupo de confianza, para una aplicación individual o para un grupo de aplicaciones que están dentro de un grupo de confianza.

Las reglas de control de aplicaciones que se definen para aplicaciones individuales o grupos de aplicaciones dentro de un grupo de confianza tienen una mayor prioridad que las reglas de control de aplicaciones que se definen para un grupo de confianza. En otras palabras, si la configuración de las reglas de control de aplicaciones para una aplicación individual o un grupo de aplicaciones dentro de un grupo de confianza es diferente de la configuración de las reglas de control de aplicaciones para el grupo de confianza, el componente Control de actividad de aplicaciones controla la actividad de la aplicación o del grupo de aplicaciones dentro del grupo de confianza en función de unas reglas de control de aplicaciones para la aplicación o el grupo de aplicaciones.

Cambiar reglas de control de aplicaciones para grupos de confianza y grupos de aplicaciones

Las reglas de control de aplicaciones óptimas para diferentes grupos de confianza se crean de forma predeterminada. La configuración de reglas para el control de grupos de aplicaciones hereda valores de la configuración de reglas de control de grupos de confianza. Puede editar las reglas predeterminadas de control de grupos de confianza y las reglas para el control de grupos de aplicaciones.

Para editar las reglas de control de grupos de confianza o las reglas para el control de grupos de aplicaciones:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de actividad de aplicaciones**.
En la parte derecha de la ventana, se muestra la configuración del componente Control de actividad de aplicaciones.
3. Haga clic en el botón **Aplicaciones**.
Este botón abre la pestaña **Reglas de Control de aplicaciones** en la ventana **Control de actividad de aplicaciones**.
4. Seleccione el grupo de confianza o grupo de aplicaciones pertinente.
5. En el menú contextual de un grupo de confianza o de un grupo de aplicaciones, seleccione **Reglas del grupo**.
Se abre la ventana **Reglas de control de grupos de aplicaciones**.
6. En la ventana **Reglas de control de grupos de aplicaciones**, lleve a cabo una de las siguientes acciones:
 - Para editar las reglas de control de un grupo de confianza o de un grupo de aplicaciones que controlan los permisos del grupo de confianza o del grupo de aplicaciones con el fin de acceder al registro del sistema operativo, a los archivos de usuario y a la configuración de la aplicación, seleccione la pestaña **Archivos y Registro del sistema**.
 - Para editar las reglas de control de un grupo de confianza o de un grupo de aplicaciones que controlan los permisos del grupo de confianza o del grupo de aplicaciones con el fin de acceder a los objetos y procesos del sistema operativo, seleccione la pestaña **Permisos**.
7. Para el recurso requerido, en la columna de la acción correspondiente, haga clic con el botón derecho del ratón para abrir el menú contextual.
8. En el menú contextual, seleccione el elemento requerido.
 - **Heredar**
 - **Autorizar**

- **Bloquear**
- **Registrar eventos**

Si está editando las reglas de control de un grupo de confianza, el elemento **Heredar** no está disponible.

9. Haga clic en **Aceptar**.

10. En la ventana **Aplicaciones**, haga clic en **Aceptar**.

11. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Edición de una regla de control de aplicaciones

De forma predeterminada, la configuración de reglas de control de aplicaciones que pertenecen a un grupo de aplicaciones o a un grupo de confianza heredan los valores de configuración de las reglas de control del grupo de confianza. Puede editar la configuración de las reglas de control de aplicaciones.

Para cambiar una regla de control de aplicaciones:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de actividad de aplicaciones**.

En la parte derecha de la ventana, se muestra la configuración del componente Control de actividad de aplicaciones.

3. Haga clic en el botón **Aplicaciones**.

Este botón abre la pestaña **Reglas de Control de aplicaciones** en la ventana **Control de actividad de aplicaciones**.

4. Seleccione la aplicación pertinente.

5. Realice una de las siguientes acciones:

- En el menú contextual de la aplicación, seleccione **Reglas de la aplicación**.
- Haga clic en el botón **Avanzado** situado en la esquina inferior derecha de la pestaña **Reglas de Control de aplicaciones**.

Se abre la ventana **Reglas de Control de aplicaciones**.

6. En la ventana **Reglas de Control de aplicaciones**, lleve a cabo una de las siguientes acciones:

- Para modificar las reglas de control de aplicaciones que rigen los permisos de la aplicación para acceder al registro del sistema operativo, a los archivos de usuario y a la configuración de la aplicación, seleccione la pestaña **Archivos y Registro del sistema**.
- Para modificar las reglas de control de aplicaciones que rigen los permisos de la aplicación para acceder a objetos y procesos del sistema operativo, seleccione la pestaña **Permisos**.

7. Para el recurso requerido, en la columna de la acción correspondiente, haga clic con el botón derecho del ratón para abrir el menú contextual.
8. En el menú contextual, seleccione el elemento requerido.
 - Heredar
 - Autorizar
 - Bloquear
 - Registrar eventos
9. Haga clic en **Aceptar**.
10. En la ventana **Aplicaciones**, haga clic en **Aceptar**.
11. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Desactivación de las descargas y actualizaciones de reglas de control de aplicaciones desde la base de datos de Kaspersky Security Network

De forma predeterminada, cuando se detecta nueva información sobre una aplicación en la base de datos de Kaspersky Security Network, Kaspersky Endpoint Security aplica las reglas de control descargadas de la base de datos del KSN para dicha aplicación. A continuación, puede editar manualmente las reglas de control de la aplicación.

Si una aplicación no se encontraba en la base de datos de Kaspersky Security Network cuando se inició por primera vez, pero la información sobre ella se agregó a la base de datos posteriormente, Kaspersky Endpoint Security actualiza automáticamente las reglas de control de esta aplicación de forma predeterminada.

Puede desactivar las descargas de reglas de control de aplicaciones desde la base de datos de Kaspersky Security Network y las actualizaciones automáticas de reglas de control para aplicaciones anteriormente desconocidas.

Para desactivar las descargas y actualizaciones de reglas de control de aplicaciones desde la base de datos de Kaspersky Security Network, lleve a cabo los siguientes pasos:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de actividad de aplicaciones**.
En la parte derecha de la ventana, se muestra la configuración del componente Control de actividad de aplicaciones.
3. Desactive la casilla de verificación **Actualizar reglas de control para aplicaciones anteriormente desconocidas desde las bases de datos de KSN**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Desactivación de la herencia de restricciones del proceso principal

La aplicación la puede iniciar el usuario u otra aplicación en ejecución. Cuando la inicia otra aplicación, se crea una secuencia de inicio, que consta de procesos principales y subprocesos.

Cuando una aplicación intenta obtener acceso a un recurso protegido, el Control de actividad de aplicaciones analiza todos los procesos principales de la aplicación para determinar si estos procesos tienen derechos para acceder al recurso protegido. Tras esto, se aplica la regla de la mínima prioridad: cuando se comparan los permisos de acceso de la aplicación con los de los procesos principales, se otorgan los permisos con la mínima prioridad a la actividad de la aplicación.

La prioridad de permisos de acceso es la siguiente:

1. **Autorizar** Este derecho de acceso tiene la máxima prioridad.
2. **Bloquear** Este derecho de acceso tiene la mínima prioridad.

Este mecanismo impide que una aplicación que no es de confianza o con permisos restringidos utilice una aplicación de confianza para realizar acciones que requieran ciertos privilegios.

Si se bloquea la actividad de una aplicación debido a la falta de permisos que se conceden a un proceso principal, puede editar esos permisos o desactivar la herencia de restricciones del proceso principal.

Para desactivar la herencia de restricciones del proceso principal:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de actividad de aplicaciones**.
En la parte derecha de la ventana, se muestra la configuración del componente Control de actividad de aplicaciones.
3. Haga clic en el botón **Aplicaciones**.
Este botón abre la pestaña **Reglas de Control de aplicaciones** en la ventana **Control de actividad de aplicaciones**.
4. Seleccione la aplicación pertinente.
5. En el menú contextual de la aplicación, seleccione **Reglas de la aplicación**.
Se abre la ventana **Reglas de Control de aplicaciones**.
6. En la ventana **Reglas de Control de aplicaciones**, seleccione la pestaña **Exclusiones**.
7. Marque la casilla de verificación **No heredar restricciones del proceso principal (aplicación)**.
8. Haga clic en **Aceptar**.
9. En la ventana **Aplicaciones**, haga clic en **Aceptar**.
10. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Exclusión de acciones de aplicaciones concretas desde las reglas de control de aplicaciones

Para excluir acciones de aplicaciones concretas desde las reglas de control de aplicaciones, haga lo siguiente:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de actividad de aplicaciones**.
En la parte derecha de la ventana, se muestra la configuración del componente Control de actividad de aplicaciones.
3. Haga clic en el botón **Aplicaciones**.
Este botón abre la pestaña **Reglas de Control de aplicaciones** en la ventana **Control de actividad de aplicaciones**.
4. Seleccione la aplicación pertinente.
5. En el menú contextual de la aplicación, seleccione **Reglas de la aplicación**.
Se abre la ventana **Reglas de Control de aplicaciones**.
6. Seleccione la pestaña **Exclusiones**.
7. Seleccione las casillas de verificación situadas junto a las acciones de las aplicaciones que no se deban supervisar.
8. Haga clic en **Aceptar**.
9. En la ventana **Aplicaciones**, haga clic en **Aceptar**.
10. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Eliminar reglas de control de aplicaciones obsoletas

De forma predeterminada, se eliminan de forma automática las reglas para aplicaciones que no se han iniciado durante 60 días. Puede modificar la duración de almacenamiento para reglas de control de aplicaciones que no se utilizan o desactivar la eliminación automática de reglas.

Para eliminar reglas de control de aplicaciones obsoletas:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de actividad de aplicaciones**.
En la parte derecha de la ventana, se muestra la configuración del componente Control de actividad de aplicaciones.
3. Realice una de las siguientes acciones:
 - Si quisiera que Kaspersky Endpoint Security eliminara reglas del control de aplicaciones sin usar, seleccione la casilla de verificación **Eliminar reglas para aplicaciones que no son iniciadas en más de** y especifique el número pertinente de días.
 - Para desactivar la eliminación automática de las reglas del control de aplicaciones sin usar, desactive la casilla de verificación **Eliminar reglas para aplicaciones que no son iniciadas en más de**.

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Protección de recursos del sistema operativo y de datos de identidad

El Control de actividad de aplicaciones administra los derechos de las aplicaciones a realizar acciones en varias categorías de los recursos del sistema operativo y de los datos de identidad.

Los especialistas de Kaspersky han creado categorías predefinidas de recursos protegidos. No puede editar ni eliminar las categorías predefinidas de recursos protegidos, ni los recursos protegidos que hay dentro de esas categorías.

Puede realizar las siguientes acciones:

- Agregar una nueva categoría de recursos protegidos.
- Agregar un nuevo recurso protegido.
- Desactivar la protección de un recurso.

Adición de una categoría de recursos protegidos

Para agregar una nueva categoría de recursos protegidos, haga lo siguiente:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de actividad de aplicaciones**.
En la parte derecha de la ventana, se muestra la configuración del componente Control de actividad de aplicaciones.
3. Haga clic en el botón **Recursos**.
Este botón abre la pestaña **Recursos protegidos** en la ventana **Control de actividad de aplicaciones**.
4. En la parte izquierda de la pestaña **Recursos protegidos**, seleccione una sección o categoría de recursos protegidos a la que desee agregar una nueva categoría de recursos protegidos.
5. Haga clic en el botón **Agregar** y, en la lista desplegable, seleccione **Categoría**.
Se abre la ventana **Categoría de recursos protegidos**.
6. En la ventana **Categoría de recursos protegidos** que se abre, introduzca un nombre para la nueva categoría de recursos protegidos.
7. Haga clic en **Aceptar**.
Aparecerá un nuevo elemento en la lista de categorías de recursos protegidos.
8. En la ventana **Control de actividad de aplicaciones**, haga clic en **Aceptar**.
9. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Después de agregar una categoría de recursos protegidos, puede editarla o eliminarla haciendo clic en los botones **Modificar** o **Eliminar** de la parte superior izquierda de la pestaña **Recursos protegidos**.

Adición de un recurso protegido

Para agregar un nuevo recurso protegido, haga lo siguiente:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de actividad de aplicaciones**.
En la parte derecha de la ventana, se muestra la configuración del componente Control de actividad de aplicaciones.
3. Haga clic en el botón **Recursos**.
Este botón abre la pestaña **Recursos protegidos** en la ventana **Control de actividad de aplicaciones**.
4. En la parte izquierda de la pestaña **Recursos protegidos**, seleccione una categoría de recursos protegidos a la que desee agregar un nuevo recurso protegido.
5. Haga clic en el **botón Agregar** y en la lista desplegable seleccionan el tipo de recurso que desea agregar:
 - **Archivo o carpeta**
 - **Clave de Registro**Se abre la ventana **Recurso protegido**.
6. En la ventana **Recurso protegido**, introduzca el nombre del recurso protegido en el campo **Nombre**.
7. Haga clic en el botón **Examinar**.
8. En la ventana que se abre, especifique la configuración necesaria según el tipo de recurso protegido que desee añadir. Haga clic en **Aceptar**.
9. En la ventana **Recurso protegido**, haga clic en **Aceptar**.
Aparecerá un nuevo elemento en la lista de recursos protegidos de la categoría seleccionada en la pestaña **Recursos protegidos**.
10. En la ventana **Control de actividad de aplicaciones**, haga clic en **Aceptar**.
11. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Después de agregar un recurso protegido, puede modificarlo o eliminarlo haciendo clic en los botones **Modificar** o **Eliminar** de la parte superior izquierda de la pestaña **Recursos protegidos**.

Desactivación de la protección de un recurso

Para desactivar la protección de un recurso, haga lo siguiente:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de actividad de aplicaciones**.

En la parte derecha de la ventana, se muestra la configuración del componente Control de actividad de aplicaciones.

3. En la parte derecha de la ventana, haga clic en el botón **Recursos**.

Este botón abre la pestaña **Recursos protegidos** en la ventana **Control de actividad de aplicaciones**.

4. Realice una de las siguientes acciones:

- En la parte izquierda de la pestaña, en la lista de recursos protegidos, seleccione el recurso para el que desee desactivar la protección y desactive la casilla de verificación situada junto a su nombre.

- Haga clic en **Exclusiones** y haga lo siguiente:

a. En la ventana **Exclusiones**, haga clic en el botón **Agregar**. En la lista desplegable, seleccione el tipo de recurso que desee agregar a la lista de exclusiones de protección mediante el componente Control de actividad de aplicaciones: **Archivo o carpeta** o **Clave de Registro**.

Se abre la ventana **Recurso protegido**.

b. En la ventana **Recurso protegido**, introduzca el nombre del recurso protegido en el campo **Nombre**.

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

d. En la ventana que se abre, especifique la configuración necesaria en función del tipo de recurso protegido que desee agregar a la lista de exclusiones de protección mediante el componente Control de actividad de aplicaciones.

e. Haga clic en **Aceptar**.

f. En la ventana **Recurso protegido**, haga clic en **Aceptar**.

Aparecerá un nuevo elemento en la lista de recursos que se han excluido de la protección en el componente Control de actividad de aplicaciones.

Después de agregar un recurso a la lista de exclusiones de protección mediante el componente Control de actividad de aplicaciones, puede editarlo o eliminarlo haciendo clic en los botones **Modificar** o **Eliminar** de la parte superior de la ventana **Exclusiones**.

g. En la ventana **Exclusiones**, haga clic en **Aceptar**.

5. En la ventana **Control de actividad de aplicaciones**, haga clic en **Aceptar**.

6. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Control de vulnerabilidades

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security se instala en un equipo con Microsoft Windows para servidores de archivos.

Esta sección contiene información sobre Control de vulnerabilidades e instrucciones sobre cómo activar o desactivar el componente.

Acerca del Control de vulnerabilidades

El componente Control de vulnerabilidades ejecuta un análisis en tiempo real de vulnerabilidades de aplicaciones que están en ejecución en el equipo o iniciadas por el usuario. Cuando se activa el componente Control de vulnerabilidades, no es necesario iniciar la tarea [Análisis de vulnerabilidades](#). Este análisis es importante cuando nunca se ha llevado a cabo la [tarea Análisis de vulnerabilidades](#) de las aplicaciones instaladas en el equipo del usuario o si se llevó a cabo hace mucho tiempo.

Activación y desactivación del Control de vulnerabilidades

El componente Control de vulnerabilidades está desactivado de forma predeterminada. Si es necesario, puede activar el Control de vulnerabilidades.

Existen dos formas de activar o desactivar el componente:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

Para activar o desactivar Control de vulnerabilidades en la pestaña Protección y control de la ventana principal de la aplicación:

1. Abra la [ventana principal de la aplicación](#).

2. Seleccione la pestaña **Protección y control**.

3. Haga clic en la sección **Control de Endpoint**.



Se abre la sección **Control de Endpoint**.

4. Haga clic con el botón derecho para mostrar el menú contextual de la línea con información sobre el componente Control de vulnerabilidades.



Se abre un menú para seleccionar acciones sobre los componentes.

5. Realice una de las siguientes acciones:

- Para activar Control de vulnerabilidades, seleccione **Iniciar**.

El icono de estado del componente , que se muestra a la izquierda en la línea **Control de vulnerabilidades**, cambia al icono .

- Para desactivar Control de vulnerabilidades, seleccione **Detener**.

El icono de estado del componente , que se muestra a la izquierda en la línea **Control de vulnerabilidades**, cambia al icono .

Para activar o desactivar Control de vulnerabilidades en la ventana de configuración de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione **Control de vulnerabilidades**.
En la parte derecha de la ventana, se muestra la configuración del componente Control de vulnerabilidades.
3. En la parte derecha de la ventana, seleccione una de las siguientes acciones:
 - Si desea que Kaspersky Endpoint Security inicie un análisis de vulnerabilidades de aplicaciones en ejecución en el equipo o iniciadas por el usuario, seleccione la casilla de verificación **Activar Control de vulnerabilidades**.
 - Si no desea que Kaspersky Endpoint Security inicie un análisis de vulnerabilidades de aplicaciones en ejecución en el equipo o iniciadas por el usuario, desactive la casilla de verificación **Activar Control de vulnerabilidades**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Control de dispositivos

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security se instala en un equipo con [Microsoft Windows para servidores de archivos](#).

Esta sección contiene información sobre Control de dispositivos e instrucciones sobre cómo configurar los parámetros del componente.

Acerca del Control de dispositivos

El Control de dispositivos garantiza la seguridad de los datos confidenciales gracias a una restricción del acceso de usuarios a dispositivos que se instalan en el equipo o se conectan a él, incluidos:

- Dispositivos de almacenamiento de datos (discos duros, unidades extraíbles, unidades de cinta, unidades de CD/DVD)
- Herramientas de transferencia de datos (módems y tarjetas de red externas)
- Dispositivos diseñados para convertir datos en copias impresas (impresoras)
- Buses de conexión (conocidos también simplemente como "buses"), que corresponden a interfaces para conectar dispositivos a equipos (como USB, FireWire e infrarrojos)

El Control de dispositivos gestiona el acceso del usuario a dispositivos mediante la aplicación de [reglas de acceso a dispositivos](#), conocidas también como "reglas de acceso", y [reglas de acceso a buses de conexión](#), conocidas también como "reglas de acceso a buses".

Activación y desactivación del Control de dispositivos

De forma predeterminada, Control de dispositivos está activado. Si es necesario, puede desactivar el Control de dispositivos.

Existen dos formas de activar o desactivar el componente:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

*Para activar o desactivar Control de dispositivos en la pestaña **Protección y control** de la ventana principal de la aplicación:*

1. Abra la ventana principal de la aplicación.
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Control de Endpoint**.
Se abre la sección **Control de Endpoint**.

4. Haga clic con el botón derecho para que aparezca el menú contextual de la línea con información sobre el componente Control de dispositivos.

Se abre un menú para seleccionar acciones sobre los componentes.

5. Realice una de las siguientes acciones:

- Para activar Control de dispositivos, seleccione **Iniciar** en el menú.
- Para desactivar Control de dispositivos, seleccione **Detener** en el menú.

Para activar o desactivar Control de dispositivos en la ventana de configuración de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de dispositivos**.

En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.

3. Realice una de las siguientes acciones:

- Si quiere activar Control de dispositivos, seleccione la casilla de verificación **Activar Control de dispositivos**.
- Si quiere desactivar Control de dispositivos, desactive la casilla de verificación **Activar Control de dispositivos**.

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Acerca de las reglas de acceso a dispositivos y a buses de conexión

Una regla de acceso a dispositivos es una combinación de parámetros que definen las siguientes funciones del componente Control de dispositivos:

- Permitir el acceso para usuarios o grupos de usuarios seleccionados a tipos específicos de dispositivos durante períodos determinados de tiempo.

Puede seleccionar un usuario o un grupo de usuarios y crear una planificación de acceso a dispositivos para ellos.

- Definir el derecho para leer el contenido de los dispositivos de memoria.
- Definir el derecho para editar el contenido de los dispositivos de memoria.

De forma predeterminada, las reglas de acceso se crean para todos los tipos de dispositivos en la clasificación del componente Control de dispositivos. Dichas reglas conceden acceso completo a los dispositivos para todos los usuarios en todo momento, si se permite el acceso a los buses de conexión de los tipos respectivos de dispositivos.

La regla de acceso a bus de conexión permite o bloquea el acceso al bus de conexión.

Las reglas que permiten el acceso a los buses se crean de forma predeterminada para todos los buses de conexión presentes en la clasificación del componente Control de dispositivos.

No puede crear ni eliminar reglas de acceso a dispositivos ni reglas de acceso a bus de conexión; únicamente puede editarlas.

Acerca de dispositivos de confianza

Los *dispositivos de confianza* son dispositivos a los que los usuarios especificados en la configuración de dispositivos de confianza tienen acceso total en todo momento.

Puede realizar las siguientes acciones con los dispositivos de confianza:

- Agregar un dispositivo a la lista de dispositivos de confianza.
- Cambiar el usuario o el grupo de usuarios con autorización para acceder al dispositivo de confianza.
- Eliminar un dispositivo a la lista de dispositivos de confianza.

Si ha agregado un dispositivo a la lista de dispositivos de confianza y ha creado una regla de acceso para ese tipo de dispositivo que bloquea o restringe el acceso, Kaspersky Endpoint Security decide si conceder acceso al dispositivo en función de su presencia en la lista de dispositivos de confianza. La presencia en la lista de dispositivos de confianza tiene una prioridad superior a una regla de acceso.

Decisiones estándar sobre el acceso a dispositivos

Kaspersky Endpoint Security toma una decisión sobre si permitir el acceso a un dispositivo después de que el usuario conecte un dispositivo al equipo.

Decisiones estándar sobre el acceso a dispositivos

No.	Condiciones iniciales	Pasos intermedios que se deben dar hasta que se toma una decisión sobre el acceso al dispositivo			Decisión sobre el acceso al dispositivo
		Comprobación de si el dispositivo está incluido en la lista de dispositivos de confianza	Comprobación del acceso al dispositivo en función de la regla de acceso	Comprobación del acceso al dispositivo en función de la regla de acceso al bus	
1	El dispositivo no está presente en la clasificación del dispositivo del componente Control de dispositivos.	No incluido en la lista de dispositivos de confianza.	Ninguna regla de acceso.	No sujeto a análisis.	Acceso autorizado.
2	El dispositivo es de confianza.	Incluido en la lista de dispositivos de confianza.	No sujeto a análisis.	No sujeto a análisis.	Acceso autorizado.
3	Acceso al dispositivo está permitido.	No incluido en la lista de dispositivos de confianza.	Acceso autorizado.	No sujeto a análisis.	Acceso autorizado.

4	El acceso al dispositivo depende del bus.	No incluido en la lista de dispositivos de confianza.	El acceso depende del bus.	Acceso autorizado.	Acceso autorizado.
5	El acceso al dispositivo depende del bus.	No incluido en la lista de dispositivos de confianza.	El acceso depende del bus.	Acceso bloqueado.	Acceso bloqueado.
6	Acceso al dispositivo está permitido. No se encuentra ninguna regla de acceso al bus.	No incluido en la lista de dispositivos de confianza.	Acceso autorizado.	Ninguna regla de acceso al bus.	Acceso autorizado.
7	El acceso al dispositivo está bloqueado.	No incluido en la lista de dispositivos de confianza.	Acceso bloqueado.	No sujeto a análisis.	Acceso bloqueado.
8	No se ha encontrado ninguna regla de acceso al dispositivo ni al bus.	No incluido en la lista de dispositivos de confianza.	Ninguna regla de acceso.	Ninguna regla de acceso al bus.	Acceso autorizado.
9	No hay ninguna regla de acceso al dispositivo.	No incluido en la lista de dispositivos de confianza.	Ninguna regla de acceso.	Acceso autorizado.	Acceso autorizado.
10	No hay ninguna regla de acceso al dispositivo.	No incluido en la lista de dispositivos de confianza.	Ninguna regla de acceso.	Acceso bloqueado.	Acceso bloqueado.

Puede editar la regla de acceso al dispositivo después de conectarse al dispositivo. Si el dispositivo está conectado y la regla de acceso permite el acceso a él, pero más adelante edita la regla de acceso y bloquea el acceso, Kaspersky Endpoint Security bloquea el acceso la próxima vez que se solicita desde el dispositivo cualquier operación con archivos (visualización del árbol de carpetas, lectura, escritura). Un dispositivo sin sistema de archivos solo se bloquea la próxima vez que se conecta el dispositivo.

Si un usuario del equipo donde se ha instalado Kaspersky Endpoint Security debe solicitar el acceso a un dispositivo que el usuario cree que se bloqueó por equivocación, envíe al usuario las [instrucciones para solicitar acceso](#).

Edición de una regla de acceso a dispositivos

Según el tipo de dispositivo, es posible modificar diversos ajustes de acceso, como la lista de usuarios que reciben acceso al dispositivo, la planificación del acceso y el acceso permitido o bloqueado.

Para editar la regla de acceso a un dispositivo:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de dispositivos**.
En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.
3. En la parte derecha de la ventana, seleccione la pestaña **Tipos de dispositivos**.

La pestaña **Tipos de dispositivos** contiene reglas de acceso a todos los dispositivos incluidos en la clasificación del componente Control de dispositivos.

4. Seleccione la regla de acceso que quiera editar.
5. Haga clic en el botón **Modificar**. Este botón solo está disponible para tipos de dispositivos que tienen un sistema de archivos.

Se abre la ventana **Configuración de la regla de acceso al dispositivo**.

De forma predeterminada, una regla de acceso al dispositivo concede a los usuarios acceso total al tipo de dispositivos especificado en cualquier momento. En la lista **Usuarios y/o grupos de usuarios**, esta regla de acceso contiene el grupo **Todos**. En la tabla **Derechos del grupo de usuarios seleccionado por planificaciones de acceso**, esta regla de acceso contiene la **Planificación predeterminada** de acceso a los dispositivos, con los derechos para llevar a cabo todo tipo de operaciones con ellos.

6. Edite la configuración de la regla de acceso al dispositivo:
 - a. Seleccione un usuario y/o grupo de usuarios de la lista **Usuarios y/o grupos de usuarios**.
Para editar la lista **Usuarios y/o grupos de usuarios**, utilice los botones **Agregar**, **Modificar** y **Eliminar**.
 - b. En la tabla **Derechos del grupo de usuarios seleccionado por planificaciones de acceso**, configure la planificación de acceso a los dispositivos para los usuarios y/o grupos de usuarios seleccionados. Para ello, seleccione las casillas de verificación junto a los nombres de las planificaciones de acceso para los dispositivos que quiera usar en la regla de acceso a dispositivos que se va a editar.
Para editar la lista de planificaciones de acceso a los dispositivos, utilice los botones **Crear**, **Modificar**, **Copiar** y **Eliminar** en la tabla **Derechos del grupo de usuarios seleccionado por planificaciones de acceso**.
 - c. Para cada planificación del acceso a los dispositivos utilizados en la regla que se edita, especifique las operaciones permitidas cuando se trabaja con dispositivos. Para ello, en la tabla **Derechos del grupo de usuarios seleccionado por planificaciones de acceso**, seleccione las casillas de verificación en las columnas con los nombres de las operaciones pertinentes.
 - d. Haga clic en **Aceptar**.

Después de editar los ajustes predeterminados de una regla de acceso al dispositivo, el ajuste del acceso al tipo de dispositivo de la columna **Acceso** de la tabla que aparece en la pestaña **Tipos de dispositivos** se cambia al valor *Restringir por las reglas*.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Agregar o excluir archivos al registro del evento o desde él

El registro de eventos solo está disponible para las operaciones con archivos en unidades extraíbles.

Para activar o desactivar el registro de eventos:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de dispositivos**.

En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.

3. En la parte derecha de la ventana, seleccione la pestaña **Tipos de dispositivos**.

La pestaña **Tipos de dispositivos** contiene reglas de acceso a todos los dispositivos incluidos en la clasificación del componente Control de dispositivos.

4. Seleccione **Unidades extraíbles** en la tabla de dispositivos.

El botón **Registro** pasa a estar disponible en la parte superior de la tabla.

5. Haga clic en el botón **Inicio de sesión**.

Esto abre la ventana **Configuración de inicio de sesión**.

6. Realice una de las siguientes acciones:

- Si desea activar el registro del borrado de archivos y escribir operaciones en unidades extraíbles, seleccione la casilla de verificación **Activar escritura en informe**.

Kaspersky Endpoint Security guardará un evento en el registro de actividades y enviará un mensaje al servidor de administración de Kaspersky Security Center siempre que el usuario realice operaciones de escritura o borrado con archivos en unidades extraíbles.

- Si no, desactive la casilla de verificación **Activar registro**.

7. Especifique qué operaciones se deben registrar. Para ello, siga uno de estos pasos:

- Si desea que Kaspersky Endpoint Security registre todos los eventos, seleccione la casilla de verificación **Guardar información sobre todos los archivos**.

- Si desea que Kaspersky Endpoint Security registre únicamente la información sobre archivos de un formato específico, en la sección **Filtrar formatos de archivo**, seleccione las casillas de verificación situadas junto a los formatos de archivo pertinentes.

8. Especifique qué acciones de los usuarios de Kaspersky Endpoint Security se deben registrar como eventos. Para ello:

a. En la sección **Usuarios**, haga clic en el botón **Seleccionar**.

Se abre la ventana estándar **Seleccionar usuarios o grupos** en Microsoft Windows.

b. Especifique o modifique la lista de usuarios y grupos de usuarios.

Cuando los usuarios especificados en la sección **Usuarios** escriben en archivos ubicados en unidades extraíbles o eliminan archivos de unidades extraíbles, Kaspersky Endpoint Security guarda la información sobre esas operaciones en el registro de eventos y envía un mensaje al servidor de administración de Kaspersky Security Center.

9. En la ventana **Configuración de inicio de sesión**, haga clic en **Aceptar**.

10. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Puede ver eventos asociados con archivos en unidades extraíbles en la Consola de administración de Kaspersky Security Center, en el espacio de trabajo del nodo **Servidor de administración**, en la pestaña **Eventos**. Para que los eventos se muestren en el registro de eventos local de Kaspersky Endpoint Security, debe seleccionar la casilla de verificación **Operación de archivo realizada** en la [configuración de notificaciones](#) para el componente Control de dispositivos.

Agregar una red Wi-Fi a la lista de confianza

Puede permitir que los usuarios se conecten a redes Wi-Fi que considera seguras, como una red Wi-Fi corporativa. Para ello, debe agregar la red a la lista de redes Wi-Fi de confianza. Control de dispositivos bloqueará el acceso a todas las redes Wi-Fi excepto las especificadas en la lista de confianza.

Para agregar una red Wi-Fi a la lista de confianza:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de dispositivos**.

En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.

3. En la parte derecha de la ventana, seleccione la pestaña **Tipos de dispositivos**.

La pestaña **Tipos de dispositivos** contiene reglas de acceso a todos los dispositivos incluidos en la clasificación del componente Control de dispositivos.

4. En la columna **Acceso** situada junto al dispositivo **Wi-Fi**, haga clic con el botón derecho del ratón para abrir el menú contextual.

5. Seleccione la opción **Bloquear con excepciones**.

6. En la lista de dispositivos, seleccione **Wi-Fi** y haga clic en el botón **Editar**.

Esto abre la ventana **Redes Wi-Fi de confianza**.

7. Haga clic en el botón **Agregar**.

Esto abre la ventana **Red Wi-Fi de confianza**.

8. En la ventana **Red Wi-Fi de confianza**:

- En el campo **Nombre de red**, especifique el nombre de la red Wi-Fi que desea agregar a la lista de confianza.
- En la lista desplegable **Tipo de autenticación**, seleccione el tipo de autenticación utilizada al conectarse a la red Wi-Fi de confianza.
- En la lista desplegable **Tipo de cifrado**, seleccione el tipo de cifrado usado para asegurar el tráfico de la red Wi-Fi de confianza.
- En el campo **Comentario**, puede especificar cualquier información sobre la red Wi-Fi que se ha agregado.

Una red Wi-Fi se considera de confianza si sus ajustes coinciden con todos los que se especifican en la regla.

9. En la ventana **Red Wi-Fi de confianza**, haga clic en **Aceptar**:

10. En la ventana **Redes Wi-Fi de confianza**, haga clic en **Aceptar**.

Edición de una regla de acceso a bus de conexión

Para editar una regla de acceso a bus de conexión:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de dispositivos**.

En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.

3. Seleccione la pestaña **Buses de conexión**.

La pestaña **Buses de conexión** muestra las reglas de acceso para todos los buses de conexión clasificados en el componente Control de dispositivos.

4. Seleccione la regla de bus de conexión que desee editar.

5. Cambie el valor del parámetro de acceso:

- Para permitir el acceso a un bus de conexión, haga clic en la columna **Acceso** para abrir el menú contextual y seleccione **Autorizar**.
- Para bloquear el acceso a un bus de conexión, haga clic en la columna **Acceso** para abrir el menú contextual y seleccione **Bloquear**.

6. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Acciones con dispositivos de confianza

Esta sección contiene información sobre acciones con dispositivos de confianza.

Adición de un dispositivo a la lista de confianza en la interfaz de la aplicación

De forma predeterminada, al agregar un dispositivo a la lista de dispositivos de confianza, a todos los usuarios (el grupo de usuarios Todos) se les concede acceso a este dispositivo.

Para agregar un dispositivo a la lista de confianza en la interfaz de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de dispositivos**.

En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.

3. En la parte derecha de la ventana, seleccione la pestaña **Dispositivos de confianza**.

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

Se abre la ventana **Seleccionar dispositivos de confianza**.

5. Seleccione la casilla de verificación situada junto al nombre del dispositivo que desee agregar a la lista de dispositivos de confianza.

La lista de la columna **Dispositivos** depende del valor que se seleccione en la lista desplegable **Mostrar dispositivos conectados**.

6. Haga clic en el botón **Seleccionar**.

Se abre la ventana **Seleccionar usuarios o grupos** en Microsoft Windows.

7. En la ventana **Seleccionar usuarios o grupos** de Microsoft Windows, especifique los usuarios o los grupos de usuarios cuyos dispositivos seleccionados Kaspersky Endpoint Security reconoce como de confianza.

Los nombres de los usuarios o grupos de usuarios especificados en la ventana **Seleccionar usuarios o grupos de usuarios** de Microsoft Windows se muestran en el campo **Permitido a usuarios y/o grupos de usuarios**.

8. En la ventana **Seleccionar dispositivos de confianza**, haga clic en **Aceptar**.

En la tabla, en la pestaña **Dispositivos de confianza** de la ventana de configuración del componente **Control de dispositivos**, aparece una línea y muestra los parámetros del dispositivo de confianza que se ha agregado.

9. Repita los pasos 4-7 por cada dispositivo que quiera agregar a la lista de dispositivos de confianza para los usuarios o grupos de usuarios especificados.

10. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Adición de dispositivos a la lista de confianza según el modelo o el ID del dispositivo

De forma predeterminada, al agregar un dispositivo a la lista de dispositivos de confianza, a todos los usuarios (el grupo de usuarios Todos) se les concede acceso a este dispositivo.

Para agregar dispositivos a la lista de confianza según el modelo o el ID del dispositivo:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea crear una lista de dispositivos de confianza.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Control de Endpoint**, seleccione la subdivisión **Control de dispositivos**.
7. En la parte derecha de la ventana, seleccione la pestaña **Dispositivos de confianza**.
8. Haga clic en el botón **Agregar**.

Se abre el menú contextual del botón.
9. En el menú contextual del botón **Agregar**, lleve a cabo una de las siguientes acciones:
 - Seleccione el botón **Dispositivos por ID** si desea seleccionar dispositivos con ID únicos conocidos que se agregarán a la lista de dispositivos de confianza.
 - Seleccione la opción **Dispositivos por modelo** para agregar a la lista los dispositivos de confianza cuyos VID (ID del proveedor) y PID (ID del producto) se conozcan.

10. En la ventana que se abre, en la lista desplegable **Tipo de dispositivo** seleccione el tipo de dispositivos que mostrar en la tabla a continuación.
11. Haga clic en el botón **Actualizar**.

La tabla muestra una lista de dispositivos para los cuales se conocen los ID o modelos de dispositivo y que pertenecen al tipo seleccionado en la lista desplegable **Tipo de dispositivo**.
12. Seleccione las casillas de verificación junto a los nombres de los dispositivos que quiera agregar a la lista de dispositivos de confianza.
13. Haga clic en el botón **Seleccionar**.

Se abre la ventana **Seleccionar usuarios o grupos** en Microsoft Windows.
14. En la ventana **Seleccionar usuarios o grupos** de Microsoft Windows, especifique los usuarios o los grupos de usuarios cuyos dispositivos seleccionados Kaspersky Endpoint Security reconoce como de confianza.

Los nombres de los usuarios o grupos de usuarios especificados en la ventana **Seleccionar usuarios o grupos de usuarios** de Microsoft Windows se muestran en el campo **Permitido a usuarios y/o grupos de usuarios**.
15. Haga clic en **Aceptar**.

Las líneas que aparecen con los parámetros de los dispositivos de confianza que se han añadido aparecen en la tabla de la pestaña **Dispositivos de confianza**.
16. Para guardar los cambios, haga clic en **Aceptar** o **Aplicar**.

Adición de dispositivos a la lista de confianza según la máscara del ID de dispositivo

De forma predeterminada, al agregar un dispositivo a la lista de dispositivos de confianza, a todos los usuarios (el grupo de usuarios Todos) se les concede acceso a este dispositivo.

Los dispositivos se pueden agregar a la lista de confianza según la máscara de su ID solamente en la consola de administración de Kaspersky Security Center.

Para agregar dispositivos a la lista de confianza según la máscara de su ID:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea crear una lista de dispositivos de confianza.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.

6. En la sección **Control de Endpoint**, seleccione la subdivisión **Control de dispositivos**.
7. En la parte derecha de la ventana, seleccione la pestaña **Dispositivos de confianza**.
8. Haga clic en el botón **Agregar**.
Se abre el menú contextual del botón.
9. En el menú contextual del botón **Agregar**, seleccione el elemento de **Dispositivos por máscara de ID**.
Se abre la ventana **Agregar dispositivos de confianza por máscara de ID**.
10. En la ventana **Agregar dispositivos de confianza por máscara de ID**, introduzca la máscara para los ID de dispositivo en el campo **Máscara**.
11. Haga clic en el botón **Seleccionar**.
Se abre la ventana **Seleccionar usuarios o grupos** en Microsoft Windows.
12. En la ventana **Seleccionar usuarios o grupos** de Microsoft Windows, especifique los usuarios o los grupos de usuarios que Kaspersky Endpoint Security reconoce como dispositivos de confianza cuyos modelos o ID coinciden con la máscara especificada.

Los nombres de los usuarios o grupos de usuarios especificados en la ventana **Seleccionar usuarios o grupos de usuarios** de Microsoft Windows se muestran en el campo **Permitido a usuarios y/o grupos de usuarios**.
13. Haga clic en **Aceptar**.
En la tabla, en la pestaña **Dispositivos de confianza** de la ventana de configuración del componente **Control de dispositivos**, aparece una línea con la configuración de la regla para agregar dispositivos a la lista de dispositivos de confianza mediante la máscara de sus ID.
14. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Configuración del acceso de usuario a un dispositivo de confianza

De forma predeterminada, al agregar un dispositivo a la lista de dispositivos de confianza, a todos los usuarios (el grupo de usuarios Todos) se les concede acceso a este dispositivo. Puede configurar el acceso de los usuarios (o grupos de usuarios) a un dispositivo de confianza.

Para configurar el acceso de los usuarios a un dispositivo de confianza:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de dispositivos**.
En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.
3. En la parte derecha de la ventana, seleccione la pestaña **Dispositivos de confianza**.
4. En la lista de dispositivos de confianza, seleccione un dispositivo para el cual desea modificar las reglas de acceso.
5. Haga clic en el botón **Modificar**.
Se abre la ventana **Configuración de la regla de acceso al dispositivo de confianza**.
6. Haga clic en el botón **Seleccionar**.

Se abre la ventana **Seleccionar usuarios o grupos** en Microsoft Windows.

7. En la ventana **Seleccionar usuarios o grupos** de Microsoft Windows, especifique los usuarios o los grupos de usuarios cuyos dispositivos seleccionados Kaspersky Endpoint Security reconoce como de confianza.
8. Haga clic en **Aceptar**.
Los nombres de los usuarios o grupos de usuarios especificados en la ventana **Seleccionar usuarios o grupos de usuarios** de Microsoft Windows se muestran en el campo **Permitido a usuarios y/o grupos de usuarios** de la ventana **Configuración de la regla de acceso al dispositivo de confianza**.
9. Haga clic en **Aceptar**.
10. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Eliminación de un dispositivo de la lista de dispositivos de confianza

Para quitar un dispositivo de la lista de dispositivos de confianza:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de dispositivos**.
En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.
3. En la parte derecha de la ventana, seleccione la pestaña **Dispositivos de confianza**.
4. Seleccione el dispositivo que desee quitar de la lista de dispositivos de confianza.
5. Haga clic en el botón **Eliminar**.
6. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Kaspersky Endpoint Security toma una decisión sobre el acceso a un dispositivo que haya quitado de la lista de dispositivos de confianza en función de las reglas de acceso a dispositivos y las reglas de acceso a bus de conexión.

Edición de plantillas de mensajes de Control de dispositivos

Cuando el usuario intenta acceder a un dispositivo bloqueado, Kaspersky Endpoint Security muestra un mensaje que afirma que el acceso al dispositivo está bloqueado o que una operación con los contenidos del dispositivo está prohibida. Si el usuario cree que el acceso al dispositivo se bloqueó por error o que una operación con contenidos del dispositivo se prohibió por error, el usuario puede enviar un mensaje al administrador de la red corporativa local haciendo clic en el enlace del mensaje mostrado sobre la acción bloqueada.

Hay plantillas disponibles para mensajes sobre el acceso bloqueado a dispositivos o sobre operaciones prohibidas con los contenidos del dispositivo, así como para mensajes enviados al administrador. Puede modificar las plantillas de los mensajes.

Para editar la plantilla para mensajes de Control de dispositivos:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control de dispositivos**.

En la parte derecha de la ventana, se muestra la configuración del componente Control de dispositivos.

3. En la parte derecha de la ventana, haga clic en el botón **Plantillas**.

Se abre la ventana **Plantillas de mensajes**.

4. Realice una de las siguientes acciones:

- Para modificar la plantilla del mensaje sobre el acceso bloqueado a un dispositivo o sobre una operación prohibida con los contenidos del dispositivo, seleccione la pestaña **Bloqueo**.
- Para modificar la plantilla del mensaje que se envía al administrador de la LAN, seleccione la pestaña **Mensaje al administrador**.

5. Edite la plantilla del mensaje. También puede usar los botones siguientes: **Variable**, **Predeterminado** y **Enlace** (este botón solo está disponible en la pestaña **Bloqueo**).

6. Haga clic en **Aceptar**.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Obtención de acceso a un dispositivo bloqueado

Estas instrucciones están destinadas a los usuarios de equipos cliente donde se haya instalado Kaspersky Endpoint Security.

La función de Kaspersky Endpoint Security que ofrece acceso temporal a un dispositivo se encuentra disponible únicamente cuando Kaspersky Endpoint Security funciona de acuerdo con la directiva de Kaspersky Security Center y esta función se ha activado en la configuración de directivas (consulte la *Guía del administrador de Kaspersky Security Center*).

Para solicitar acceso a un dispositivo bloqueado desde la ventana de configuración del componente Control de dispositivos:

1. En la ventana principal de la aplicación, seleccione la pestaña **Protección y control**.

2. Haga clic en la sección **Control de Endpoint**.

Se abre la sección **Control de Endpoint**.

3. Haga clic con el botón derecho para que aparezca el menú contextual de la línea con información sobre el componente Control de dispositivos.

Se abre un menú para seleccionar acciones sobre los componentes.

4. Haga clic en el botón **Acceso al dispositivo**.

Se abre la ventana **Solicitar acceso al dispositivo**.

5. En la lista de dispositivos conectados, seleccione aquél al que quiere tener acceso.

6. Haga clic en el botón **Generar archivo de solicitud de acceso**.

Esto abre la ventana **Creación de archivo de solicitud de acceso**.

7. En el campo **Duración del acceso**, especifique el período de tiempo durante el que desea disponer de acceso al dispositivo.
8. Haga clic en el botón **Guardar**.
Esto abre la ventana estándar **Guardar archivo de solicitud de acceso** de Microsoft Windows.
9. En la ventana **Guardar archivo de solicitud de acceso** de Microsoft Windows, seleccione la carpeta en la que desee guardar el archivo de solicitud de acceso del dispositivo y haga clic en el botón **Guardar**.
10. Envíe el archivo de solicitud de acceso del dispositivo al administrador de la red de área local.
11. Reciba el archivo de claves de acceso del dispositivo que le facilite el administrador de la red de área local.
12. En la ventana **Solicitar acceso al dispositivo**, haga clic en el botón **Activar clave de acceso**.
Se abre la ventana estándar **Abrir clave de acceso** de Microsoft Windows.
13. En la ventana **Abrir clave de acceso** de Microsoft Windows, seleccione el archivo de claves de acceso del dispositivo que le facilitó el administrador de la red de área local y haga clic en el botón **Abrir**.
Se abre la ventana **Activación de la clave de acceso para el dispositivo** y muestra información sobre el acceso proporcionado.
14. En la ventana **Activación de la clave de acceso para el dispositivo**, haga clic en **Aceptar**.

Para solicitar acceso a un dispositivo bloqueado haciendo clic en el enlace del mensaje que informa de que el dispositivo está bloqueado:

1. En la ventana con el mensaje que informa de que un dispositivo o bus de conexión está bloqueado, haga clic en el enlace **Solicitar acceso**.
Esto abre la ventana **Creación de archivo de solicitud de acceso**.
2. En el campo **Duración del acceso**, especifique el período de tiempo durante el que desea disponer de acceso al dispositivo.
3. Haga clic en el botón **Guardar**.
Esto abre la ventana estándar **Guardar archivo de solicitud de acceso** de Microsoft Windows.
4. En la ventana **Guardar archivo de solicitud de acceso** de Microsoft Windows, seleccione la carpeta en la que desee guardar el archivo de solicitud de acceso del dispositivo y haga clic en el botón **Guardar**.
5. Envíe el archivo de solicitud de acceso del dispositivo al administrador de la red de área local.
6. Reciba el archivo de claves de acceso del dispositivo que le facilite el administrador de la red de área local.
7. En la ventana **Solicitar acceso al dispositivo**, haga clic en el botón **Activar clave de acceso**.
Se abre la ventana estándar **Abrir clave de acceso** de Microsoft Windows.
8. En la ventana **Abrir clave de acceso** de Microsoft Windows, seleccione el archivo de claves de acceso del dispositivo que le facilitó el administrador de la red de área local y haga clic en el botón **Abrir**.
Se abre la ventana **Activación de la clave de acceso para el dispositivo** y muestra información sobre el acceso proporcionado.
9. En la ventana **Activación de la clave de acceso para el dispositivo**, haga clic en **Aceptar**.

El período de tiempo para el que se concede acceso al dispositivo puede ser diferente a la cantidad de tiempo que solicitó. El acceso al dispositivo se concede para el período de tiempo que especifique el administrador de la red de área local al generar el código de acceso al dispositivo.

Crear una clave para acceder a un dispositivo bloqueado mediante Kaspersky Security Center

Para conceder a un usuario acceso temporal a un dispositivo bloqueado, se requiere una clave de acceso al dispositivo. Puede crear una clave de acceso mediante Kaspersky Security Center.

Con el fin de crear una clave de acceso para un dispositivo bloqueado:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En la lista de equipos cliente, seleccione el equipo de un usuario que necesite obtener acceso temporal a un dispositivo bloqueado.
5. En el menú contextual del equipo, seleccione **Conceder acceso a dispositivos y datos en modo offline**.
Se abre la ventana **Conceder acceso a dispositivos y datos en modo offline**.
6. Seleccione la pestaña **Control de dispositivos**.
7. En la pestaña **Control de dispositivos**, haga clic en el botón **Examinar**.
Se abre la ventana estándar **Seleccionar archivo de solicitud de acceso** de Microsoft Windows.
8. En la ventana **Seleccionar archivo de solicitud de acceso**, seleccione el archivo de solicitud de acceso que haya recibido del usuario y haga clic en el botón **Abrir**.
Control de dispositivos muestra los detalles del dispositivo bloqueado al que el usuario ha solicitado acceso.
9. Especifique el valor del parámetro **Duración del acceso**.
Este parámetro define el período de tiempo durante el que concede al usuario acceso al dispositivo bloqueado. El valor predeterminado es el que especificó el usuario al crear el archivo de solicitud de acceso.
10. Especifique el valor del parámetro **Período de activación**.
Este parámetro define el período durante el cual el usuario puede activar el acceso al dispositivo bloqueado mediante la clave de acceso proporcionada.
11. Haga clic en el botón **Guardar**.
Esto abre la ventana estándar **Guardar clave de acceso** de Microsoft Windows.
12. Seleccione la carpeta de destino en la que desee guardar el archivo que contiene la clave de acceso al dispositivo bloqueado.
13. Haga clic en el botón **Guardar**.

Control Web

Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Microsoft Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security se instala en un equipo con [Microsoft Windows para servidores de archivos](#).

Esta sección contiene información sobre Control Web e instrucciones sobre cómo configurar los parámetros del componente.

Acerca de Control Web

Control Web permite que los usuarios de la LAN controlen acciones restringiendo o bloqueando el acceso a los recursos web.

Un recurso web es una página web o varias páginas web, o bien un sitio web o varios que cuentan con una característica común.

El Control Web ofrece las siguientes opciones:

- Ahorro de tráfico.
El tráfico se controla mediante la restricción o el bloqueo de descargas de archivos multimedia, o la restricción o el bloqueo del acceso a recursos web que no están relacionados con las responsabilidades del trabajo de los usuarios.
- Delimitación del acceso mediante categorías de contenido de recursos web.
Para ahorrar tráfico y reducir las pérdidas potenciales provocadas por el mal uso del tiempo de los empleados, puede restringir o bloquear el acceso a categorías específicas de recursos web (por ejemplo, bloquear el acceso a recursos web que pertenecen a la categoría "Medios de comunicación por Internet").
- Control centralizado del acceso a recursos web.
Cuando se utiliza Kaspersky Security Center, está disponible la configuración personal y de un grupo para el acceso a recursos web.

Todas las restricciones y bloqueos que se aplican al acceso a recursos web se implementan como [reglas de acceso a recursos web](#).

Activación y desactivación de Control Web

De forma predeterminada, Control Web está activado. Si es necesario, puede desactivar el Control Web.

Existen dos formas de activar o desactivar el componente:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

*Para activar o desactivar Control Web en la pestaña **Protección y control** de la ventana principal de la aplicación:*

1. Abra la ventana principal de la aplicación.
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Control de Endpoint**.
Se abre la sección **Control de Endpoint**.
4. Haga clic con el botón derecho para que aparezca el menú contextual de la línea con información sobre el componente Control Web.
Se abre un menú para seleccionar acciones sobre los componentes.
5. Realice una de las siguientes acciones:
 - Para activar Control Web, seleccione **Iniciar** en el menú.
 - Para desactivar Control Web, seleccione **Detener** en el menú.

Para activar o desactivar Control Web en la ventana de configuración de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control Web**.
En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. Realice una de las siguientes acciones:
 - Si quiere activar Control Web, seleccione la casilla de verificación **Activar Control Web**.
 - Si quiere desactivar Control Web, desactive la casilla de verificación **Activar Control Web**.

Si se desactiva Control Web, Kaspersky Endpoint Security no controla el acceso a los recursos de Internet.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Categorías de contenido de recursos web

Las categorías de contenido de recursos web (más adelante denominadas también "categorías") indicadas a continuación se han seleccionado para describir todo lo posible los bloques de datos alojados por recursos web, teniendo en cuenta sus características funcionales y temáticas. El orden en el que las categorías aparecen en esta lista no refleja la importancia ni el predominio relativo de dichas categorías en Internet. Los nombres de las categorías son provisionales y solo se utilizan a efectos de los productos y los sitios web de Kaspersky. Dichos nombres no reflejan necesariamente el significado implícito por ley. Un recurso web puede pertenecer a varias categorías simultáneamente.

Contenido para adultos

Esta categoría incluye los recursos web siguientes:

- Recursos web que contienen fotos o vídeos que muestran los órganos genitales de seres humanos o de criaturas humanoides, así como actos de cópula sexual o masturbación practicados por seres humanos o criaturas humanoides.

- Recursos web que contienen textos, incluidos materiales literarios o artísticos, que describen órganos genitales de seres humanos o de criaturas humanoides, así como actos de cópula sexual o masturbación practicados por seres humanos o criaturas humanoides.
- Recursos web dedicados al debate del lado sexual de las relaciones humanas.

Se solapa con la categoría "Medios de comunicación por Internet".

- Recursos web que contienen materiales eróticos, trabajos que proporcionan una imagen realista del comportamiento sexual de los seres humanos, así como obras de arte concebidas para estimular la excitación sexual.
- Recursos web de medios de comunicación oficiales y comunidades en línea con una audiencia objetivo establecida, que contienen una sección especial o artículos independientes dedicados al aspecto sexual de las relaciones humanas.
- Recursos web dedicados a las perversiones sexuales.
- Recursos web que anuncian y venden artículos para su uso durante la práctica de relaciones sexuales y la estimulación de la excitación sexual, incluidos servicios de contacto y prestación de servicios sexuales como los ofrecidos a través de chats de vídeo eróticos, como "sexo telefónico" o con el envío de mensajes con contenido sexual ("sexting" o "sexo virtual").
- Recursos web con los siguientes contenidos:
 - Artículos y blogs que tratan la educación sexual, tanto de temas científicos como populares.
 - Enciclopedias médicas, en concreto las secciones sobre reproducción sexual.
 - Recursos de instituciones médicas, concretamente las secciones que versan sobre los órganos sexuales.

Software, audio, vídeo

Esta categoría incluye las subcategorías siguientes, que puede seleccionar individualmente:

- **Audio y vídeo.**

Esta subcategoría incluye recursos web que distribuyen materiales de audio y vídeo como películas, retransmisiones de eventos deportivos, grabaciones de conciertos, canciones, videoclips, vídeos, tutoriales de audio y vídeo, etc.

- **Archivos torrent.**

Esta subcategoría incluye sitios web de rastreadores de archivos torrent cuyo fin es compartir archivos de tamaño ilimitado.

- **Uso compartido de archivos.**

Esta subcategoría incluye sitios web de uso compartido de archivos, independiente de la ubicación física de los archivos distribuidos.

Alcohol, tabaco, narcóticos

Esta categoría incluye recursos web cuyo contenido se relaciona directa o indirectamente con productos alcohólicos o que contienen alcohol, tabaco, y sustancias narcóticas, psicotrópicas o tóxicas.

- Recursos web que anuncian y venden estas sustancias y accesorios para consumirlas.

Se solapa con la categoría "Comercio electrónico".

- Recursos web con instrucciones sobre cómo consumir o fabricar sustancias narcóticas, psicotrópicas o tóxicas.

Esta categoría incluye recursos web que abordan temas científicos y médicos.

Violencia

Esta categoría incluye recursos web que contienen fotos, vídeos o texto que describen actos de violencia física o psicológica contra seres humanos, o de crueldad con los animales.

- Recursos web que representan o describen escenas de ejecuciones, tortura o abuso, así como las herramientas destinadas a tales prácticas.

Se solapa con la categoría "Armas, explosivos, pirotecnia".

- Recursos web que representan o describen escenas de asesinato, lucha, agresión o violación, así como escenas en las que se abusa de seres humanos, animales u otras criaturas imaginarias o en las que se les humilla.
- Recursos web con información que incita a cometer actos que ponen en riesgo la vida o la salud, incluidos lesiones autoinfligidas y el suicidio.
- Recurso web con información que prueba o justifica la admisibilidad de la violencia o la crueldad, o que incitan a cometer actos violentos contra seres humanos o animales.
- Recursos web con imágenes especialmente realistas o descripciones de víctimas y atrocidades de guerra, conflictos armados, y choques militares, accidentes, catástrofes, desastres naturales, cataclismos industriales o sociales, o sufrimiento de los seres humanos.
- Videojuegos con escenas de violencia y crueldad, incluidos los de "tiros", "combates", "peleas", etc.

Se solapa con la categoría "Videojuegos".

Armas, explosivos, pirotecnia

Esta categoría incluye recursos web con información sobre armas, explosivos y productos pirotécnicos:

- sitios web de fabricantes y tiendas de armas, explosivos y fabricantes de productos pirotécnicos.

Se solapa con la categoría "Comercio electrónico".

- Recursos web dedicados a la fabricación o al uso de armas, explosivos y productos pirotécnicos.

- Recursos web que incluyen materiales analíticos, históricos, enciclopédicos y de producción dedicados a las armas, los explosivos y los productos pirotécnicos.

El término "armas" significa dispositivos, elementos y medios diseñados para dañar la vida o la salud de los seres humanos y los animales, así como equipos y estructuras.

Lenguaje soez

Esta categoría incluye recursos web donde se ha detectado un lenguaje soez.

Se solapa con la categoría "Contenido para adultos".

Esta categoría también incluye recursos web con materiales de carácter lingüístico y filológico que contienen un lenguaje soez como tema de estudio.

Casinos y subastas, loterías y sorteos

Esta categoría incluye recursos web que permiten que los usuarios participen económicamente en apuestas, incluso si dicha participación no es una condición obligatoria para el acceso al sitio web. Esta categoría incluye recursos web que ofrecen lo siguiente:

- Apuestas en las que los participantes deben hacer contribuciones monetarias.

Se solapa con la categoría "Videojuegos".

- Sorteos que implican apostar dinero.
- Loterías que implican la adquisición de boletos o números de lotería.
- Información que puede activar el deseo de participar en apuestas, sorteos y loterías.

Se solapa con la categoría "Comercio electrónico".

Esta categoría incluye los juegos que ofrecen participación gratuita como modo independiente, así como recursos web que anuncian activamente a los usuarios los recursos que entran en esta categoría.

Comunicaciones de red

Esta categoría incluye los recursos web que permiten a los usuarios (registrados o no) enviar mensajes personales a otros usuarios de los recursos web pertinentes o a otros servicios en línea, o agregar contenido (tanto de acceso público como restringido) a los recursos web pertinentes en determinadas condiciones. Puede seleccionar individualmente las subcategorías siguientes:

- **Chats y foros.**

Esta subcategoría incluye recursos web destinados al debate público de diversos temas mediante aplicaciones web especiales, así como recursos web diseñados para distribuir o respaldar aplicaciones de mensajería instantánea que permiten la comunicación de tiempo real.

- **Blogs.**

Esta subcategoría incluye las plataformas de blog, que son sitios web que proporcionan servicios gratuitos o de pago para crear y mantener blogs.

- **Redes sociales.**

Esta subcategoría incluye sitios web diseñados para crear, mostrar y gestionar el contacto entre personas, organizaciones y gobiernos, para el que se requiere el registro de una cuenta de usuario como condición de participación.

- **Sitios de contactos.**

Esta subcategoría incluye recursos web que funcionan como una variedad de redes sociales que proporcionan servicios de pago o gratuitos.

Se solapa con las categorías "Contenido para adultos" y "Comercio electrónico".

- **Correo electrónico basado en Web.**

Esta subcategoría incluye solo páginas de inicio de sesión de un servicio de correo electrónico y páginas de buzón que contienen correos electrónicos y datos asociados (por ejemplo, contactos personales). Esta categoría no incluye otras páginas web de un proveedor de servicios de Internet que también ofrece servicio de correo electrónico.

E-tailers, bancos y sistemas de pago

Esta categoría incluye los recursos web diseñados para cualquier transacción con fondos no monetarios mediante aplicaciones web especiales. Puede seleccionar individualmente las subcategorías siguientes:

- **Tiendas y subastas.**

Esta subcategoría incluye tiendas y subastas en línea que venden cualquier mercancía, trabajo o servicio a las personas físicas o entidades jurídicas, incluidos los sitios web de tiendas que llevan a cabo ventas exclusivamente en línea y perfiles en línea de las tiendas físicas que aceptan pagos en línea.

- **Bancos.**

Esta subcategoría incluye páginas web especializadas de bancos que ofrecen servicios bancarios en línea, incluidos las transferencias (electrónicas) entre cuentas bancarias, la creación de depósitos bancarios, la conversión de divisas, el pago de servicios de terceros, etc.

- **Sistemas de pago.**

Esta subcategoría incluye páginas web de sistemas de dinero electrónico que proporcionan acceso a la cuenta personal del usuario.

En términos técnicos, el pago puede efectuarse con tarjetas bancarias de cualquier tipo (plástico o virtual, crédito o débito, local o internacional) y con dinero electrónico. Los recursos web pueden entrar en esta categoría independientemente de si disponen de aspectos técnicos como la transmisión de datos sobre protocolo SSL, el uso de la autenticación 3D Secure, etc.

Esta categoría incluye los recursos web diseñados para reunir a empleadores y buscadores de trabajo:

- Sitios web de agencias de contratación (agencias de colocación o agencias de cazatalentos).
- Sitios web de empleadores con descripciones de puestos de trabajo disponibles y de sus ventajas.
- Portales independientes con ofertas de empleo de empleadores y agencias de contratación.
- Redes sociales profesionales que, entre otras cosas, permiten publicar o encontrar información sobre especialistas que no están buscando empleo activamente.

Se solapa con la categoría "Medios de comunicación por Internet".

Sistemas de acceso anónimos

Esta categoría incluye los recursos web que actúan como intermediario en la descarga de contenido de otros recursos web mediante aplicaciones web especiales con el fin de:

- Omitir las restricciones impuestas por un administrador de la LAN sobre el acceso a las direcciones web o a las direcciones IP.
- Acceder de forma anónima a los recursos web, incluidos aquellos recursos que rechazan específicamente las solicitudes HTTP de ciertas direcciones IP o de sus grupos (por ejemplo, las direcciones IP agrupadas por país de origen).

Esta categoría incluye ambos recursos web previstos exclusivamente para los propósitos mencionados anteriormente ("anonimizadores") y recursos web con funcionalidad técnicamente similar.

Videojuegos

Esta categoría incluye los recursos web dedicados a videojuegos de diversos géneros:

- Sitios web de los desarrolladores de videojuegos.
- Recursos web dedicados a un debate sobre videojuegos.

Se solapa con la categoría "Medios de comunicación por Internet".

- Recursos web que proporcionan la capacidad técnica para la participación en línea en juegos, con otros participantes o de forma individual, con la instalación local de aplicaciones o sin dicha instalación ("juegos de Internet").
- Recursos web diseñados para anunciar, distribuir y dar soporte a software de videojuegos.

Se solapa con la categoría "Comercio electrónico".

Religiones y asociaciones religiosas

Esta categoría incluye recursos web con materiales sobre movimientos, asociaciones y organizaciones públicos con una ideología religiosa o cualquier manifestación de culto.

- Sitios web de organizaciones religiosas oficiales en niveles diferentes, desde religiones internacionales hasta las comunidades religiosas locales.
- Sitios web de asociaciones y sociedades religiosas no registradas que emergieron históricamente como consecuencia de la división de una asociación o comunidad religiosa dominante.
- Sitios web de asociaciones y comunidades religiosas que han emergido independientemente de los movimientos religiosos tradicionales, incluido aquellos por iniciativa de un fundador específico.
- Sitios web de organizaciones interconfesionales que persiguen la cooperación entre los representantes de distintas religiones tradicionales.
- Recursos web con materiales académicos, históricos y enciclopédicos relativos a las religiones.
- Recursos web con representaciones o descripciones detalladas de la adoración como parte de los cultos religiosos, incluidos ritos y rituales que implican la adoración a Dios, a seres u objetos sobre los que se cree que tienen poderes sobrenaturales.

Medios de información

Esta categoría incluye recursos web con contenido público de noticias creado por medios de comunicación o publicaciones en línea que permiten a los usuarios agregar sus propios informes de noticias:

- Sitios web de canales de medios de comunicación oficiales.
- Sitios web que ofrecen servicios informativos con la asignación de orígenes de información oficiales.
- Sitios web que ofrecen servicios de agregación, colecciones de noticias de fuentes oficiales y no oficiales diversas.
- Sitios web donde los usuarios crean el contenido de las noticias ("sitios de noticias sociales").

Se solapa con la categoría "Medios de comunicación por Internet".

Anuncios

Esta categoría incluye los recursos web que vienen acompañados de anuncios. La información de publicidad que aparece en los banners puede distraer a los usuarios de sus actividades, al tiempo que las descargas de los banners aumentan la cantidad de tráfico.

Acerca de las reglas de acceso a recursos web

Una regla de acceso a recursos web es un conjunto de filtros y acciones que Kaspersky Endpoint Security realiza cuando el usuario visita recursos web que se describen en la regla durante el lapso de tiempo indicado en la planificación de reglas. Los filtros permiten especificar de forma precisa un conjunto de recursos web para los que el componente Control Web controla el acceso.

Están disponibles los siguientes filtros:

- **Filtrar por contenido.** Control Web categoriza los [recursos web por contenido](#) y tipo de datos. Puede controlar el acceso de los usuarios a los recursos web con tipos de datos y contenido de determinadas categorías. Cuando los usuarios visitan recursos web que pertenecen a la categoría de contenido o de tipo de dato seleccionada, Kaspersky Endpoint Security realiza la acción especificada en la regla.
- **Filtrar por direcciones de recursos web.** Puede controlar el acceso de los usuarios a todas las direcciones de recursos web, a direcciones de recursos web individuales o a grupos de direcciones de recursos web.
Si se especifica el filtro por contenido y por direcciones de recursos web, y las direcciones de recursos web o los grupos de direcciones de recursos web especificados pertenecen a las categorías de contenido o de tipo de dato seleccionadas, Kaspersky Endpoint Security no controla el acceso a todos los recursos web en dichas categorías de contenido o de tipo de datos. En lugar de ello, la aplicación controla el acceso únicamente a las direcciones de recursos web o a los grupos de direcciones de recursos web.
- **Filtrar por nombres de usuarios y grupos de usuarios.** Puede especificar los nombres de los usuarios y/o de los grupos de usuarios para los que el acceso a los recursos web esté controlado de acuerdo con la regla.
- **Planificación de reglas.** Puede especificar la planificación de reglas. La planificación de reglas determina el intervalo de tiempo durante el que Kaspersky Endpoint Security supervisa el acceso a los recursos web cubiertos por la regla.

Tras instalar Kaspersky Endpoint Security, la lista de reglas del componente Control Web deja de estar en blanco. Se predefinen dos reglas:

- La regla de tablas de estilo y escenarios, que concede acceso a todos los usuarios y en todo momento a los recursos web cuyas direcciones contienen los nombres de los archivos con las extensiones css, js o vbs. Por ejemplo: <http://www.example.com/style.css>, <http://www.example.com/style.css?mode=normal>.
- La "Regla predeterminada" que concede acceso a todos los usuarios a cualquier recurso web en todo momento.

Acciones con reglas de acceso a recursos web

Puede realizar las siguientes acciones con las reglas de acceso a recursos web:

- Agregar una nueva regla.
- Modificar una regla.
- Asignar prioridad a una regla.

La prioridad de una regla se define por la posición de la línea que contiene una breve descripción de dicha regla dentro de la tabla de reglas del acceso en la ventana de configuración del componente Control Web. Esto quiere decir que una regla que se encuentre por encima en la tabla de reglas de acceso tiene una prioridad superior que una situada por debajo.

Si el recurso web al que el usuario intenta acceder coincide con los parámetros de varias reglas, Kaspersky Endpoint Security realiza una acción de acuerdo con la regla con la máxima prioridad.

- Probar una regla.

Puede comprobar la coherencia de las reglas mediante el servicio de diagnóstico de reglas.

- Activar y desactivar una regla.

Se puede activar (estado de funcionamiento: *Activo*) o desactivar (estado de funcionamiento: *Inactivo*) una regla de acceso a recursos web. De forma predeterminada, tras crear una regla, esta se activa (estado de funcionamiento: *Activo*). Puede desactivar la regla.

- Eliminar regla

Adición y edición de reglas de acceso a recursos web

Para agregar y editar una regla de acceso a recursos web:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control Web**.
En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. Realice una de las siguientes acciones:

- Para agregar una regla, haga clic en el botón **Agregar**.
- Si desea editar una regla, seleccionar la regla en la tabla y haga clic en el botón **Editar**.

Se abre la ventana **Regla de acceso a recursos web**.

4. Especifique o edite la configuración de la regla. Para ello:
 - a. En el campo **Nombre**, introduzca o edite el nombre de la regla.
 - b. En la lista desplegable **Filtrar contenido**, seleccione la opción necesaria:
 - **Cualquier contenido**.
 - **Por categorías de contenido**.
 - **Por tipos de datos**.
 - **Por categorías de contenido y tipos de datos**.
 - c. Si se selecciona una opción distinta de **Cualquier contenido** se abren las secciones para seleccionar categorías de contenido y tipos de datos. Seleccione las casillas de verificación junto a los nombres de las categorías de contenido y de tipos de datos requeridas.
Al seleccionar la casilla de verificación junto al nombre de una categoría de contenido o de tipos de datos, Kaspersky Endpoint Security aplica la regla para controlar el acceso a los recursos web que pertenecen a las categorías de contenido o a las categorías de tipos de datos seleccionadas.
 - d. En la lista desplegable **Aplicar a direcciones**, seleccione la opción necesaria:
 - **A todas las direcciones**.
 - **A direcciones individuales**.
 - e. Si se seleccione la opción **A direcciones individuales**, se abre una sección en la que puede crear una lista de recursos web. Puede agregar o editar las direcciones de recursos web utilizando los botones **Agregar**, **Editar** y **Eliminar**.
 - f. Seleccione la casilla de verificación **Especificar usuarios y/o grupos**.
 - g. Haga clic en el botón **Seleccionar**.

Se abre la ventana **Seleccionar usuarios o grupos** en Microsoft Windows.

- h. Especifique o edite la lista de usuarios y/o grupos de usuarios para los que se permite o se bloquea el acceso a los recursos web descritos por la regla.
- i. En la lista desplegable **Acción**, seleccione la opción necesaria:
 - Si se selecciona el valor **Autorizar**, Kaspersky Endpoint Security permite el acceso a los recursos de Internet que coinciden con los parámetros de la regla.
 - Si se selecciona el valor **Bloquear**, Kaspersky Endpoint Security bloquea el acceso a los recursos de Internet que coinciden con los parámetros de la regla.
 - **Advertir**. Si se selecciona este valor, Kaspersky Endpoint Security muestra una advertencia de que un recurso web es no deseado cuando el usuario intenta acceder a recursos web que coincidan con la regla. Al usar enlaces desde el mensaje de advertencia, el usuario puede obtener acceso al recurso web solicitado.
- j. En la lista desplegable **Planificación de reglas**, seleccione el nombre de la planificación necesaria o genere una nueva planificación basada en la planificación de la regla seleccionada. Para ello:
 1. Enfrente de la lista desplegable **Planificación de reglas**, haga clic en el botón **Configuración**.
Se abre la ventana **Planificación de reglas**.
 2. Para agregar a la planificación de reglas un intervalo de tiempo durante el que la regla no se aplica, en la tabla que muestra la planificación de reglas, haga clic en las celdas de la tabla correspondientes a la hora y al día de la semana que quiera seleccionar.
El color de las celdas se vuelve gris.
 3. Para sustituir un intervalo de tiempo durante el que la regla se aplica por otro intervalo de tiempo durante el que no se aplica dicha regla, haga clic en las celdas grises de la tabla que corresponde a la hora y al día de la semana que quiera seleccionar.
El color de las celdas se vuelve verde.
 4. Haga clic en el botón **Guardar como**.
Se abre la ventana **Nombre de planificación de reglas**.
 5. Introduzca un nombre de planificación de reglas o deje el nombre predeterminado que se sugiere.
 6. Haga clic en **Aceptar**.
5. En la ventana **Regla de acceso a recursos web**, haga clic en **Aceptar**.
6. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Asignación de prioridades a reglas de acceso a recursos web

Puede asignar prioridades a cada regla de la lista de reglas, organizando las reglas de un modo determinado.

Para asignar una prioridad a una regla de acceso a un recurso web:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control Web**.
En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. En la parte derecha de la ventana, seleccione la regla para la que quiera cambiar la prioridad.
4. Utilice los botones **Subir** y **Bajar** para mover la regla al puesto que quiera en la lista de reglas.
5. Repita los pasos 3–4 para las reglas cuya prioridad quiera cambiar.
6. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Comprobación de las reglas de acceso a recursos web

Para comprobar la coherencia de las reglas de Control Web, puede probarlas. Con este fin, el componente Control Web incluye la función Diagnóstico de reglas.

Para probar las reglas de acceso a recursos web:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control Web**.
En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. En la parte derecha de la ventana, haga clic en el botón **Diagnóstico**.
Se abre la ventana **Diagnóstico de reglas**.
4. Rellene los campos de la sección **Condiciones**:
 - a. Si quiere probar las reglas que utiliza Kaspersky Endpoint Security para controlar el acceso a un recurso web específico, seleccione la casilla de verificación **Especificar dirección** e introduzca la dirección del recurso web en el campo siguiente.
 - b. Si quiere probar las reglas que Kaspersky Endpoint Security utiliza para controlar el acceso a recursos web para usuarios y grupos de usuarios especificados, especifique una lista de usuarios y grupos de usuarios.
 - c. Si quiere probar las reglas que utiliza Kaspersky Endpoint Security para controlar el acceso a recursos web de las categorías de contenido y categorías de tipos de datos especificadas, en la lista desplegable **Filtrar contenido**, seleccione la opción necesaria (**Por categorías de contenido**, **Por tipos de datos** o **Por categorías de contenido y tipos de datos**).
 - d. Si quiere probar las reglas que tienen en cuenta la hora y el día de la semana cuando se realiza un intento de acceder a los recursos web especificados en las condiciones del diagnóstico de reglas, seleccione la casilla de verificación **Incluir hora del intento de acceso**. A continuación, especifique el día de la semana y la hora.
5. Haga clic en el botón **Prueba**.

Después de que se complete la prueba, aparece un mensaje con información sobre la acción que realiza Kaspersky Endpoint Security, de acuerdo con la primera regla activada ante un intento de acceso al recurso web especificado (autorizar, bloquear o advertir). La primera regla que se activa es la primera con un rango en la lista de reglas de Control Web superior al de otras reglas que cumplen las condiciones de diagnóstico. El mensaje se muestra a la derecha del botón **Prueba**. La siguiente tabla incluye las reglas restantes activadas, en las que se especifica la acción que ha llevado a cabo Kaspersky Endpoint Security. Las reglas se incluyen en orden de prioridad decreciente.

Activación y desactivación de una regla de acceso a recursos web

Para activar o desactivar una regla de acceso a recursos web:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control Web**.
En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. En la parte derecha de la ventana, seleccione la regla que desee activar o desactivar.
4. En la columna **Estado**, haga lo siguiente:
 - Si desea activar el uso de la regla, seleccione el valor *Activo*.
 - Si desea desactivar el uso de la regla, seleccione el valor *Inactivo*.
5. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Migración de reglas de acceso a recursos web de las versiones previas de la aplicación


Cuando Service Pack 1 Maintenance Release 1 o una versión anterior de la aplicación se actualiza a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, las reglas de acceso a recursos web basadas en categorías de contenido de recursos web se migran conforme a los principios siguientes:

- Las reglas de acceso a recursos web basadas en una o varias categorías de contenido de recursos web en las listas "Foros y chats", "Correo web", y "Redes sociales" migran a la categoría de contenido de recursos web "Medios de comunicación por Internet".
- Las reglas de acceso a recursos web basadas en una o varias categorías de contenido de recursos web en las listas "Tiendas en línea" y "Sistemas de pago" migran a la categoría de contenido de recursos web "Comercio electrónico".
- Las reglas de acceso a recursos web basadas en la categoría de contenido de recursos web "Casinos y subastas" migran a la categoría de contenido "Apuestas, loterías y sorteos".
- Las reglas de acceso a recursos web basadas en la categoría "Juegos de Internet" migran a la categoría de contenido "Videojuegos".
- Las reglas de acceso a recursos web basadas en categorías de contenido de recursos web no incluidas en la lista anterior se migran sin cambios.

Exportación e importación de la lista de direcciones de recursos web


Si ha creado una lista de direcciones de recursos web en una regla de acceso a recursos web, puede exportarla a un archivo .txt. Puede importar en veces sucesivas la lista desde este archivo para evitar la creación de una nueva lista de direcciones de recursos web manualmente al configurar una regla de acceso. La opción de exportación e importación de la lista de direcciones de recursos web puede ser útil si, por ejemplo, crea reglas de acceso con parámetros similares.

Para exportar una lista de direcciones de recursos web a un archivo:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control Web**.
En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. Seleccione la regla cuya lista de direcciones de recursos web desee exportar a un archivo.
4. Haga clic en el botón **Modificar**.
Se abre la ventana **Regla de acceso a recursos web**.
5. Si solo desea exportar una parte de la lista completa de direcciones de recursos web, en lugar de la lista completa, seleccione las direcciones de recursos web necesarios requeridos.
6. A la derecha del campo con la lista de direcciones de recursos web, haga clic en el botón .
- Se abre la ventana de confirmación de la acción.
7. Realice una de las siguientes acciones:
 - Si desea exportar únicamente los elementos seleccionados de la lista de direcciones de recursos web, haga clic en el botón **Sí** de la ventana de confirmación de acción.
 - Si desea exportar todos los elementos de la lista de direcciones de recursos web, haga clic en el botón **No** de la ventana de confirmación de acción.
Se abre la ventana estándar **Guardar como** de Microsoft Office.
8. En la ventana **Guardar como** de Microsoft Windows, seleccione el archivo al que desee exportar la lista de direcciones de recursos web. Haga clic en el botón **Guardar**.

Para importar la lista de direcciones de recursos web de un archivo a una regla:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control Web**.
En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. Realice una de las siguientes acciones:
 - Si desea crear una nueva regla de acceso a recursos web, haga clic en el botón **Agregar**.
 - Seleccione la regla de acceso a recursos web que desee editar. A continuación, haga clic en el botón **Modificar**.
Se abre la ventana **Regla de acceso a recursos web**.
4. Realice una de las siguientes acciones:

- Si va a crear una nueva regla de acceso a recursos web, seleccione **A direcciones individuales** en la lista desplegable **Aplicar a direcciones**.
 - Si va a editar una regla de acceso a recursos web, vaya al paso 5 de estas instrucciones.
5. A la derecha del campo con la lista de direcciones de recursos web, haga clic en el botón .
- Si va a crear una nueva regla, se abre la ventana estándar **Abrir archivo** de Microsoft Windows.
- Si va a editar una regla, se abre una ventana para solicitarle su confirmación.
6. Realice una de las siguientes acciones:
- Si va a editar una nueva regla de acceso a recursos web, vaya al paso 7 de estas instrucciones.
 - Si va a editar una regla de acceso a recursos web, realice una de las siguientes acciones en la ventana de confirmación de acción:
 - Si desea agregar elementos importados de la lista de direcciones de recursos web a elementos existentes, haga clic en el botón **Sí**.
 - Si desea eliminar elementos existentes de la lista de direcciones de recursos web y agregar elementos importados, haga clic en el botón **No**.
- Se abre la ventana **Abrir archivo** de Microsoft Windows.
7. En la ventana **Abrir archivo** de Microsoft Windows, seleccione un archivo que contenga una lista de direcciones de recursos web para importar.
8. Haga clic en el botón **Abrir**.
9. En la ventana **Regla de acceso a recursos web**, haga clic en **Aceptar**.

Edición de máscaras para direcciones de recursos web

El uso de una *máscara para direcciones de recursos web* (también denominada "máscara de dirección") puede resultar útil si tiene que introducir varias direcciones de recursos web similares al crear una regla de acceso a recursos web. Si se elabora correctamente, una máscara de dirección puede sustituir un gran número de direcciones de recursos web.

Siga estas reglas si va a crear una máscara de dirección:

1. El carácter ***** sustituye cualquier secuencia que contenga cero caracteres o más.

Por ejemplo, si introduce la máscara de dirección ***abc***, la regla de acceso se aplica a todos los recursos web que contengan la secuencia abc. Ejemplo: http://www.example.com/page_0-9abcdef.html.

Si quiere incluir el carácter ***** en la máscara de dirección, introduzca el carácter ***** dos veces.

2. La secuencia de caracteres **www.** que se encuentra al comienzo de cualquier máscara de dirección se interpreta como ***. .**

Ejemplo: la máscara de dirección www.example.com se considera como ***.example.com**.

3. Si una máscara de dirección no comienza con el carácter *****, su contenido será equivalente al mismo contenido con el prefijo ***. .**

4. La secuencia de caracteres * . que se encuentra al principio de una máscara de dirección se interpreta como * . o como una cadena vacía.

Ejemplo: la máscara de dirección http://www.*.example.com incluye la dirección http://www2.example.com.

5. Si una máscara de dirección termina con un carácter distinto de / o * , su contenido será equivalente al mismo contenido que con el sufijo /* .

Ejemplo: la máscara de dirección http://www.example.com incluye direcciones como http://www.example.com/abc donde a, b y c son cualesquiera caracteres.

6. Si una máscara de dirección termina con el carácter / , su contenido será equivalente al mismo contenido que con el posfijo /* . .

7. La secuencia de caracteres /* al final de una máscara de dirección se considera como /* o como una cadena vacía.

8. Las direcciones de recursos web se contrastan con una máscara de dirección y se tiene en cuenta el protocolo (http o https):

- Si la máscara de dirección no contiene ningún protocolo de red, dicha máscara de dirección abarca direcciones con cualquier protocolo de red.

Ejemplo: la máscara de dirección example.com incluye las direcciones http://example.com y https://example.com.

- Si la máscara de dirección contiene un protocolo de red, dicha máscara de dirección abarca únicamente direcciones con el mismo protocolo de red que el de la máscara de dirección.

Ejemplo: la máscara de dirección http://*.example.com incluye la dirección http://www.example.com, pero no incluye https://www.example.com.

9. Una máscara de dirección entre comillas dobles se trata sin tener en cuenta ninguna sustitución adicional, excepto el carácter * si se ha incluido inicialmente en la máscara de dirección. Las reglas 5 y 7 no se aplican a las máscaras de dirección que aparezcan dentro de dobles comillas (ver ejemplos 14-18 en la siguiente tabla).

10. Durante la comparación con la máscara de dirección de un recurso web no se tienen en cuenta el nombre de usuario, la contraseña, el puerto de conexión ni la diferencia entre mayúsculas y minúsculas de los caracteres.

Ejemplos de cómo utilizar reglas para crear máscaras de dirección

No.	Máscara de dirección	Dirección de un recurso web para verificar	Es la dirección que abarca la máscara de dirección	Comentario
1	*.example.com	http://www.123example.com	No	Consulte la regla 1.
2	*.example.com	http://www.123.example.com	Sí	Consulte la regla 1.
3	*example.com	http://www.123example.com	Sí	Consulte la regla 1.
4	*example.com	http://www.123.example.com	Sí	Consulte la regla 1.
5	http://www.*.example.com	http://www.123example.com	No	Consulte la regla 1.
6	www.example.com	http://www.example.com	Sí	Consulte las reglas 2 y 1.
7	www.example.com	https://www.example.com	Sí	Consulte las reglas 2

				y 1.
8	http://www*.example.com	http://123.example.com	Sí	Consulte las reglas 2, 4 y 1.
9	www.example.com	http://www.example.com/abc	Sí	Consulte las reglas 2, 5 y 1.
10	example.com	http://www.example.com	Sí	Consulte las reglas 3 y 1.
11	http://example.com/	http://example.com/abc	Sí	Consulte la regla 6.
12	http://example.com/*	http://example.com	Sí	Consulte la regla 7.
13	http://example.com	https://example.com	No	Consulte la regla 8.
14	"example.com"	http://www.example.com	No	Consulte la regla 9.
15	"http://www.example.com"	http://www.example.com/abc	No	Consulte la regla 9.
16	"*.example.com"	http://www.example.com	Sí	Consulte las reglas 1 y 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Sí	Consulte las reglas 1 y 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Sí	Consulte las reglas 9 y 8.
19	www.example.com/abc/123	http://www.example.com/abc	No	Una máscara de dirección contiene más información aparte de la dirección de un recurso web.

Edición de plantillas de mensajes de Control Web

Dependiendo del tipo de acción seleccionado en las propiedades de las reglas de Control Web, Kaspersky Endpoint Security muestra un mensaje de uno de los siguientes tipos cuando los usuarios intentan acceder a recursos de Internet (la aplicación sustituye una página HTML por un mensaje para la respuesta para el servidor HTTP):

- Mensaje de advertencia. Este mensaje advierte al usuario de que no se recomienda visitar el recurso web o de que este infringe la directiva corporativa de seguridad. Kaspersky Endpoint Security muestra un mensaje de advertencia si se selecciona la opción **Advertir** en la lista desplegable **Acción** de los ajustes de la regla que describe este recurso web.

Si el usuario cree que la advertencia es un error, este puede hacer clic en el enlace de la advertencia para enviar un mensaje generado previamente al administrador de la red de área local.

- Mensaje que informe del bloqueo de un recurso web. Kaspersky Endpoint Security muestra un mensaje que informa de que se ha bloqueado un recurso web, si se selecciona la opción **Bloquear** en la lista desplegable **Acción** en los ajustes de la regla que describe este recurso web.

Si el usuario cree que el recurso web está bloqueado por error, este puede hacer clic en el enlace del mensaje que informa del bloqueo del recurso web para enviar un mensaje generado previamente y enviárselo al administrador de la red de área local.

Se proporcionan plantillas especiales para un mensaje de advertencia, el mensaje que informe de que se ha bloqueado un recurso web y el mensaje que se envía al administrador de la LAN. Puede modificar su contenido.

Para cambiar la plantilla de mensajes de Control Web:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Control de Endpoint**, seleccione el apartado **Control Web**.
En la parte derecha de la ventana, se muestra la configuración del componente Control Web.
3. En la parte derecha de la ventana, haga clic en el botón **Plantillas**.
Se abre la ventana **Plantillas de mensajes**.
4. Realice una de las siguientes acciones:
 - Si quiere editar la plantilla del mensaje que advierte al usuario de que no debe visitar un recurso web, seleccione la pestaña **Advertencia**.
 - Si quiere modificar la plantilla del mensaje que informa al usuario de que el acceso a un recurso web está bloqueado, seleccione la pestaña **Bloqueo**.
 - Para editar la plantilla del mensaje que se envía al administrador, seleccione la pestaña **Mensaje al administrador**.
5. Edite la plantilla del mensaje. También puede utilizar la lista desplegable **Variable**, así como los botones **Predeterminado** y **Enlace** (este botón no está disponible en la pestaña **Mensaje al administrador**).
6. Haga clic en **Aceptar**.
7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Sensor de endpoint de KATA

La configuración del componente Sensor de endpoint de KATA solo está disponible en la consola de administración de Kaspersky Security Center. Para utilizar este componente, debe instalar el complemento de administración.

Esta sección contiene información sobre el sensor de endpoint de KATA e instrucciones sobre cómo activar o desactivar este componente.

Acerca del sensor de endpoint de KATA

El *sensor de endpoint de KATA* es un componente de la plataforma Kaspersky Anti Targeted Attack. Esta solución está destinada a la detección rápida de amenazas como ataques dirigidos.

Este componente se instala en los equipos cliente. En estos equipos, el componente supervisa continuamente los procesos, las conexiones de red activas y los archivos que se modifican, y traslada esta información a la plataforma Kaspersky Anti Targeted Attack.

La funcionalidad del componente está disponible con estos sistemas operativos:

- Microsoft Windows 7 Professional / Enterprise / Ultimate edición x86 SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate edición x64 SP1.
- Microsoft Windows 8,1 Enterprise edición x86, Microsoft Windows 8,1 Enterprise edición x64.
- Microsoft Windows 10 Pro / Enterprise edición x86, Microsoft Windows 10 Pro / Enterprise edición x64.
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1.
- Microsoft Windows Server 2012 Standard / Foundation / Essentials edición x64, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials edición x64.
- Microsoft Windows Server 2016

Para obtener más información acerca de la plataforma Kaspersky Anti Targeted Attack que no se proporcione en este documento, consulte la ayuda de la plataforma Kaspersky Anti Targeted Attack.

Las conexiones entrantes a los equipos con el componente Sensor de endpoint de KATA se deben permitir desde el servidor de la plataforma Kaspersky Anti Targeted Attack directamente, sin un servidor proxy.

Activación y desactivación del componente Sensor de endpoint de KATA

Para activar o desactivar el componente Sensor de endpoint de KATA:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración pertinente para el que desea editar la configuración de directivas.

3. En el espacio de trabajo, seleccione la pestaña **Directivas**.

4. Seleccione la directiva necesaria.

5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:

- En el menú contextual de la directiva, seleccione **Propiedades**.
- Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.

6. En la sección **Configuración avanzada**, seleccione el apartado **Sensor de endpoint de KATA**.

7. Realice una de las siguientes acciones:

- Si desea activar Sensor de endpoint de KATA, seleccione la casilla de verificación **Sensor de endpoint de KATA**.
- Si desea desactivar Sensor de endpoint de KATA, desactive la casilla de verificación **Sensor de endpoint de KATA**.

8. Si seleccionó la casilla de verificación **Sensor de endpoint de KATA** durante el paso anterior, en el campo **Dirección del Servidor**, especifique la dirección del servidor de Kaspersky Anti Targeted Attack Platform que consta de las partes siguientes:

- a. Nombre del protocolo
- b. Dirección IP o nombre de dominio completo (FQDN) del servidor
- c. Ruta al Recopilador de eventos de Windows en el servidor

9. Haga clic en **Aceptar**.

10. Aplique la directiva.

Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

Cifrado de datos

Si se instala Kaspersky Endpoint Security en un equipo en el que se ejecuta Microsoft Windows para estaciones de trabajo, todos los datos de funcionalidad de cifrado están completamente disponibles. Si se instala Kaspersky Endpoint Security en un equipo en el que se ejecuta [Microsoft Windows para servidores de archivos](#), solo está disponible el uso de cifrado de disco mediante tecnología de Cifrado de unidad BitLocker.

Esta sección contiene información acerca del cifrado y descifrado de discos duros, de unidades extraíbles y de los archivos y las carpetas de las unidades del equipo local, y ofrece instrucciones para configurar y realizar el cifrado y el descifrado de datos con Kaspersky Endpoint Security, así como el complemento de administración de Kaspersky Security.

Si no hay acceso a datos cifrados, consulte las instrucciones especiales para trabajar con datos cifrados ([Trabajar con archivos con una funcionalidad de cifrado de archivos limitada](#), [Trabajar con dispositivos cifrados si no existe acceso a estos](#)).

Activación de la visualización de la configuración del cifrado de la directiva de Kaspersky Security Center

Para activar la visualización de la configuración del cifrado de la directiva de Kaspersky Security Center:

1. Abra la consola de administración de Kaspersky Security Center.
2. En el menú contextual del nodo **Servidor de administración - <nombre del equipo>** del árbol de la consola de administración, seleccione **Ver** → **Configuración de la interfaz**.
Se abre la ventana **Configuración de la interfaz**.
3. En la ventana **Configuración de la interfaz**, seleccione la casilla de verificación **Mostrar cifrado y protección de datos**.
4. Haga clic en **Aceptar**.

Acerca del cifrado de datos

Kaspersky Endpoint Security le permite cifrar las carpetas y los archivos almacenados en las unidades locales y extraíbles, o las unidades extraíbles y los discos duros por completo. El cifrado de datos minimiza el riesgo de filtraciones de información que se puede producir en caso de pérdida o robo del equipo portátil, unidad extraíble o disco duro, o cuando usuarios y aplicaciones no autorizados acceden a los datos.

Si la licencia ha caducado, la aplicación no cifra datos nuevos, y los datos cifrados antiguos permanecen cifrados y disponibles para su uso. En este caso, para cifrar nuevos datos se requiere activar el programa con una nueva licencia que permita el uso de cifrado.

Si la licencia ha caducado, si no se ha cumplido el Contrato de licencia de usuario final, si se ha eliminado la clave o si se ha desinstalado Kaspersky Endpoint Security, no se garantiza que los archivos cifrados previamente se encuentren cifrados. La razón es que algunas aplicaciones, como Microsoft Office Word, crean una copia temporal de los archivos cuando se modifican. Cuando se guarda el archivo original, la copia temporal sustituye al archivo original. Por lo tanto, en un equipo que no disponga de funcionalidad de cifrado, o un equipo en la que esta funcionalidad no sea accesible, el archivo permanece sin cifrar.

Kaspersky Endpoint Security ofrece las siguientes características de protección de datos:

- **Cifrado de los archivos de las unidades del equipo local.** Puede [compilar listas de archivos](#) por extensión o grupos de extensiones y listas de carpetas almacenadas en las unidades del equipo local, así como crear [reglas para el cifrado de los archivos creados por aplicaciones específicas](#). Después de aplicar una directiva de Kaspersky Security Center, Kaspersky Endpoint Security cifra y descifra los archivos siguientes:
 - Archivos agregados individualmente a listas para su cifrado y descifrado.
 - Archivos almacenados en carpetas agregados a listas para su cifrado y descifrado.
 - Archivos creados por aplicaciones separadas.

Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

- **Cifrado de unidades extraíbles.** Puede especificar una regla de cifrado predeterminada para que la aplicación lleve a cabo la misma acción en todas las unidades extraíbles o especificar reglas de cifrado de unidades extraíbles particulares.

La prioridad de la regla de cifrado predeterminada es más baja que la de las reglas de cifrado creadas para unidades extraíbles particulares. La prioridad de las reglas de cifrado creadas para las unidades extraíbles del modelo de dispositivo especificado es más baja que la de las reglas de cifrado creadas para las unidades extraíbles cuyo ID de dispositivo es el especificado.

Para seleccionar una regla de cifrado de los archivos de una unidad extraíble, Kaspersky Endpoint Security comprueba si se conocen el modelo de dispositivo y el ID. A continuación, la aplicación realiza una de las siguientes operaciones:

- Si se conoce el modelo de dispositivo únicamente, la aplicación utiliza la regla de cifrado (si existe alguna) creada para las unidades extraíbles del modelo de dispositivo especificado.
- Si se conoce el ID de dispositivo únicamente, la aplicación utiliza la regla de cifrado (si existe alguna) creada para las unidades extraíbles con el ID de dispositivo especificado.
- Si se conocen el modelo de dispositivo y el ID, la aplicación utiliza la regla de cifrado (si existe alguna) creada para las unidades extraíbles con el ID de dispositivo especificado. Si no existe tal regla, pero sí una regla de cifrado creada para unidades extraíbles con el modelo de dispositivo específico, la aplicación aplica esta regla. Si no se especifica ninguna regla de cifrado para el ID de dispositivo específico del modelo de dispositivo concreto, la aplicación aplica la regla de cifrado predeterminada.
- Si no se conocen el modelo de dispositivo ni el ID de dispositivo, la aplicación utiliza la regla de cifrado predeterminada.

La aplicación le permite preparar una unidad extraíble para que pueda utilizar los datos cifrados que contiene en modo portátil. Una vez que active el modo portátil, puede acceder a los archivos cifrados de las unidades extraíbles conectadas al equipo sin la necesidad de disponer de la funcionalidad de cifrado.

La aplicación realiza la acción que se especifica en la regla de cifrado cuando se aplica la directiva de Kaspersky Security Center.

- **Gestión de reglas de acceso de las aplicaciones a los archivos cifrados.** Para cualquier aplicación, puede crear una regla de acceso a archivos cifrados que bloquee el acceso a archivos de este tipo o lo permita solo como ciphertext, que es una secuencia de caracteres que se obtiene cuando se aplica el cifrado.
- **Creación de archivos comprimidos cifrados.** Puede crear archivos comprimidos cifrados y proteger el acceso a dichos archivos mediante una contraseña. Solo se puede acceder al contenido de los archivos comprimidos cifrados por medio de las contraseñas con las cuales se protegió el acceso a dichos archivos comprimidos. Dichos archivos comprimidos se pueden transmitir de forma segura a través de redes o por medio de unidades extraíbles.
- **Cifrado de discos duros.** Puede seleccionar una tecnología de cifrado: Cifrado de disco de Kaspersky o Cifrado de unidad BitLocker (en adelante, también denominada "BitLocker").

BitLocker es una tecnología que forma parte del sistema operativo Windows. Si un equipo está dotado de un módulo de plataforma segura (TPM), BitLocker lo utiliza para almacenar claves de recuperación que proporcionan acceso a un disco duro cifrado. Cuando el equipo se inicia, BitLocker solicita las claves de recuperación del disco duro desde el módulo de plataforma segura y desbloquea la unidad. Puede configurar el uso de una contraseña y un código PIN para acceder a las claves de recuperación.

Puede especificar la regla de cifrado de discos duros predeterminada y crear una lista de discos duros que se deben excluir del cifrado. Kaspersky Endpoint Security cifra los discos duros sector por sector cuando se aplica la directiva de Kaspersky Security Center. La aplicación cifra todas las particiones lógicas de los discos duros de forma simultánea. Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

Después de que se hayan cifrado los discos duros del sistema, en el siguiente inicio de sesión en el equipo, el usuario debe autenticarse en el [Agente de autenticación](#) antes de que se pueda acceder a los discos duros y cargar el sistema operativo. Esto requiere la introducción de la contraseña del token o la tarjeta inteligente conectada al equipo, o bien el nombre de usuario y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red de área local que utilice las tareas de gestión de las cuentas del Agente de autenticación. Estas cuentas se basan en las cuentas de Microsoft Windows con las que los usuarios inician sesión en el sistema operativo. Puede administrar las cuentas del Agente de autenticación y utilizar la tecnología de inicio de sesión único (SSO) que le permite iniciar sesión en el sistema operativo de forma automática con el usuario y la contraseña del Agente de autenticación.

Kaspersky Endpoint Security duplica las cuentas del Agente de autenticación si crea una copia de respaldo del equipo y cifra los datos de este, y, a continuación, restaura la copia de respaldo del equipo y vuelve a cifrar dichos datos. Para eliminar las cuentas duplicadas, debe usar la herramienta klmover con la clave `dupfix`. La utilidad klmover se incluye en la compilación de Kaspersky Security Center. Puede leer más sobre su funcionamiento en la *Guía de administrador de Kaspersky Security Center*.

Cuando se actualiza la versión de la aplicación a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, no se guarda la lista de cuentas del Agente de autenticación.

Solo se puede acceder a discos duros cifrados en los equipos en los que se haya instalado Kaspersky Endpoint Security con la [funcionalidad de cifrado de discos duros](#). Esta precaución minimiza el riesgo de fuga de datos de un disco duro cifrado cuando se intenta acceder a él desde el exterior de la red de área local de la compañía.

Para cifrar discos duros y unidades extraíbles, puede utilizar la función **Cifrar únicamente el espacio en disco utilizado**. Se recomienda utilizar esta función solo para dispositivos nuevos que no se hayan utilizado anteriormente. Si va a aplicar cifrado a un dispositivo que ya está en uso, se recomienda que cifre el dispositivo completo. Esto garantiza que se protegen todos los datos, incluso los datos eliminados que todavía podrían contener información recuperable.

Antes comenzar el cifrado, Kaspersky Endpoint Security obtiene el mapa de los sectores del sistema de archivos. La primera oleada de cifrado incluye los sectores que están ocupados por archivos en el momento en que se inicia el cifrado. La segunda oleada de cifrado incluye los sectores que se escribieron después de que comenzara el cifrado. Una vez que el cifrado se ha completado, todos los sectores que contienen datos están cifrados.

Una vez que el cifrado se ha completado y un usuario elimina un archivo, los sectores que almacenaban el archivo eliminado vuelven a estar disponibles para almacenar nueva información a nivel del sistema de archivos, pero permanecen cifrados. De este modo, como los nuevos archivos se escriben en un dispositivo nuevo durante el inicio del cifrado habitual con la función **Cifrar únicamente el espacio en disco utilizado** activada en el equipo, después de algún tiempo todos los sectores se cifrarán.

El servidor de administración de Kaspersky Security Center que haya controlado el equipo durante el cifrado proporciona los datos necesarios para descifrar archivos. Se puede obtener el acceso de las siguientes maneras si el equipo con los archivos cifrados se encuentra bajo el control de otro servidor de administración por cualquier motivo y si no se ha accedido nunca a los archivos cifrados:

- Solicite acceso a los objetos cifrados al administrador de la red de área local.
- Restaurar datos en dispositivos cifrados por medio de la Utilidad de restauración.
- Mediante una copia de respaldo, restaure la configuración del servidor de administración de Kaspersky Security Center que haya controlado el equipo durante el cifrado y utilice esta configuración en el servidor de administración que ahora controla el equipo con los archivos cifrados.

La aplicación crea archivos de servicio durante el cifrado. Se requiere alrededor de un dos o tres por ciento del espacio libre no fragmentado en el disco duro para almacenarlos. Si no hay bastante espacio libre no fragmentado en el disco duro, el cifrado no comenzará hasta que se libere suficiente.

No se admite la compatibilidad entre la funcionalidad de cifrado de Kaspersky Endpoint Security y Kaspersky Anti-Virus para UEFI. El cifrado de los discos duros de los equipos en los que está instalado Kaspersky Anti-Virus para UEFI impide el uso de Kaspersky Anti-Virus para UEFI.

Limitaciones de funcionalidad del cifrado

La creación de nuevas particiones en los discos duros cifrados, así como el formateo de las particiones existentes de los discos duros cifrados, pueden causar la pérdida de datos en estos discos duros.

El cifrado del disco duro con la tecnología Cifrado de disco de Kaspersky no está disponible para los discos duros que no cumplan los requisitos de software y hardware.

Kaspersky Endpoint Security no admite las configuraciones siguientes:

- El cargador de arranque se ubica en una unidad mientras que el sistema operativo se halla en una unidad diferente.
- El sistema contiene el software integrado del estándar UEFI 32.
- Intel® Rapid Start Technology y las unidades que constan de una partición de hibernación incluso cuando Intel® Rapid Start Technology está desactivada.

- Unidades de disco en formato MBR con más de cuatro particiones ampliadas.
- Archivo de intercambio ubicado en una unidad de disco que no pertenece al sistema.
- Sistema multiarranque con varios sistemas operativos instalados simultáneamente.
- Particiones dinámicas (solo se admiten las particiones principales).
- Unidades de disco con menos del 2 % de espacio libre en disco no fragmentado.
- Unidades de disco con un tamaño del sector distinto de 512 bytes o 4096 bytes que emulan 512 bytes.
- Unidades híbridadas.

Cambio del algoritmo de cifrado

El algoritmo de cifrado utilizado por Kaspersky Endpoint Security para el cifrado de datos depende de las bibliotecas de cifrado que se incluyen en el kit de distribución.

Para cambiar el algoritmo de cifrado:

1. Descifre objetos que Kaspersky Endpoint Security cifró antes de comenzar a cambiar el algoritmo del cifrado.

Después de que el algoritmo del cifrado se modifique, los objetos que se cifraron anteriormente dejarán de estar disponibles.

2. [Elimine Kaspersky Endpoint Security](#).
3. [Instale Kaspersky Endpoint Security](#) desde el kit de distribución que contiene bibliotecas de cifrado para números de bits diferentes.

Activación de la tecnología de inicio de sesión único (SSO)

La tecnología de inicio de sesión único (SSO) es incompatible con proveedores externos de credenciales de cuentas.

Para activar la tecnología de inicio de sesión único (SSO):

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea activar la tecnología de inicio de sesión único (SSO).
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:

- En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Configuración común de cifrado**.
7. En el apartado **Configuración común de cifrado**, haga clic en el botón **Configurar** en la sección **Configuración de contraseña**.
- Así, se abre la pestaña **Agente de autenticación** de la ventana **Configuración de contraseñas de cifrado**.
8. Seleccione la casilla de verificación **Utilizar la tecnología de inicio de sesión único (SSO)**.
9. Haga clic en **Aceptar**.
10. Para guardar los cambios, en la ventana **Propiedades: <Nombre de directiva>**, haga clic en **Aceptar**.
11. Aplique la directiva.
- Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

Consideraciones especiales para el cifrado de archivos

Al usar la funcionalidad de cifrado de archivos, deberá tener en cuenta los siguiente puntos:

- La directiva de Kaspersky Security Center con la configuración preestablecida para el cifrado extraíble de la unidad se forma para un grupo específico de equipos administrados. Por lo tanto, el resultado de la aplicación de la directiva del cifrado/descifrado de archivos a las unidades extraíbles depende del equipo al cual esté conectada la unidad extraíble.
- Kaspersky Endpoint Security no cifra ni descifra archivos almacenados en las unidades extraíbles cuyo estado sea de solo lectura.
- Kaspersky Endpoint Security cifra y descifra los archivos de las carpetas predeterminadas solo para los perfiles de usuario local del sistema operativo. Kaspersky Endpoint Security no cifra ni descifra los archivos de las carpetas predeterminadas de los perfiles de usuario en itinerancia, de los perfiles de usuario obligatorio, de los perfiles de usuario temporal ni de las carpetas redirigidas. La lista de carpetas estándar recomendadas por Kaspersky para el cifrado incluye las carpetas siguientes:
 - Mis documentos.
 - Favoritos.
 - Cookies.
 - Escritorio.
 - Archivos temporales de Internet Explorer.
 - Archivos temporales.
 - Archivos de Outlook

- Kaspersky Endpoint Security no cifra los archivos ni las carpetas cuando el cifrado pueda dañar el sistema operativo y las aplicaciones instaladas. Por ejemplo, los siguientes archivos y carpetas con todas las carpetas anidadas se encuentran en la lista de exclusiones del cifrado:
 - %WINDIR%.
 - %PROGRAMFILES%, %PROGRAMFILES (X86)%.
 - Archivos de registro de Windows.

No se puede ver ni modificar la lista de exclusiones del cifrado. Los archivos y las carpetas de la lista de exclusiones del cifrado se pueden agregar a la lista de cifrado, pero no se cifrarán durante la tarea de cifrado de archivos y carpetas.

- Los siguientes tipos de dispositivo son compatibles como unidades extraíbles:
 - Medios de datos conectados por medio del puerto USB
 - Discos duros conectados por medio de los puertos USB y FireWire
 - Unidades SSD conectadas por medio de los puertos USB y FireWire

Cifrado de los archivos de las unidades del equipo local

El cifrado de archivos de las unidades del equipo local está disponible si Kaspersky Endpoint Security se instala en un equipo con Microsoft Windows para estaciones de trabajo. El cifrado de archivos de las unidades del equipo local no está disponible si Kaspersky Endpoint Security se instala en un equipo con [Microsoft Windows para servidores de archivos](#).

Esta sección presenta el cifrado de los archivos de las unidades del equipo local y proporciona instrucciones para configurar y realizar el cifrado de los archivos de las unidades del equipo con Kaspersky Endpoint Security y el complemento de consola de Kaspersky Endpoint Security.

Cifrado de los archivos de las unidades del equipo local

Para cifrar los archivos de las unidades de disco locales:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea configurar el descifrado de archivos de unidades de disco locales.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.

- Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de archivos y carpetas**.
 7. En la parte derecha de la ventana, seleccione la pestaña **Cifrado**.
 8. En la lista desplegable **Modo de cifrado**, seleccione el elemento **Reglas predeterminadas**.
 9. En la pestaña **Cifrado**, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione uno de los elementos siguientes:
 - a. Seleccione el elemento **Carpetas predeterminadas** para agregar archivos desde carpetas de perfiles de usuario locales sugeridos por expertos de Kaspersky a una regla de cifrado.
Se abre la ventana **Seleccionar carpetas predeterminadas**.
 - b. Seleccione el elemento **Carpeta personalizada** para agregar una ruta de la carpeta introducida manualmente a una regla de cifrado.
Se abre la ventana **Agregar carpeta personalizada**.
 - c. Seleccione el elemento **Archivos por extensión** para agregar extensiones de archivo a una regla de cifrado. Kaspersky Endpoint Security cifra los archivos de todas las unidades locales del equipo que tienen las extensiones especificadas.
Se abre la ventana **Agregar/modificar la lista de extensiones de archivo**.
 - d. Seleccione el elemento **Archivos por grupos de extensiones** para agregar grupos de extensiones de archivo a una regla de cifrado. Kaspersky Endpoint Security cifra archivos cuyas extensiones se incluyen en los grupos de extensiones de todas las unidades de disco locales del equipo.
Se abre la ventana **Seleccionar grupos de extensiones de archivos**.
 10. Para guardar los cambios, en la ventana **Propiedades: <Nombre de directiva>**, haga clic en **Aceptar**.
 11. Aplique la directiva.
Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

Una vez que se aplica la directiva, Kaspersky Endpoint Security cifra los archivos incluidos en la regla de cifrado que no se incluyen en la [regla de descifrado](#).

Si un mismo archivo se ha agregado a la regla de cifrado y a la de descifrado, Kaspersky Endpoint Security no cifra este archivo si está descifrado y descifra el archivo si está cifrado.

Kaspersky Endpoint Security cifra archivos no cifrados si sus propiedades (ruta de archivo / nombre de archivo / extensión de archivo) siguen cumpliendo los criterios de la regla de cifrado después de la modificación.

Kaspersky Endpoint Security pospone el cifrado de archivos abiertos hasta que se cierren.

Cuando el usuario crea un nuevo archivo cuyas propiedades cumplen los criterios de la regla de cifrado, Kaspersky Endpoint Security cifra el archivo en cuanto se abre.

Si mueve un archivo cifrado a otra carpeta de la unidad local, el archivo se mantiene cifrado, sin considerar si la carpeta se incluye o no en la regla de cifrado.

Creación de reglas de acceso a archivos cifrados para aplicaciones

Para crear reglas de acceso a archivos cifrados para aplicaciones:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración pertinente para el que desea configurar las reglas de acceso a archivos cifrados para aplicaciones.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de archivos y carpetas**.
7. En la lista desplegable **Modo de cifrado**, seleccione el elemento **Reglas predeterminadas**.

Las reglas de acceso solo se aplican cuando se está en el modo **Reglas predeterminadas**. Tras aplicar reglas de acceso en el modo **Mediante reglas**, si cambia al modo **Dejar sin modificar**, Kaspersky Endpoint Security ignorará todas las reglas de acceso. Todas las aplicaciones tendrán acceso a todos los archivos cifrados.

8. En la parte derecha de la ventana, seleccione la pestaña **Reglas para aplicaciones**.
9. Si desea seleccionar aplicaciones exclusivamente desde la lista de Kaspersky Security Center, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione el elemento **Aplicaciones de la lista de Kaspersky Security Center**.

Se abre la ventana **Agregar aplicaciones de la lista de Kaspersky Security Center**.

Haga lo siguiente:

- a. Especifique los filtros para restringir la lista de aplicaciones de la tabla. Para ello, especifique los valores de los parámetros **Aplicación**, **Proveedor** y **Período agregado**, así como todas las casillas de verificación de la sección **Grupo**.
- b. Haga clic en el botón **Actualizar**.

La tabla muestra las aplicaciones que cumplen los filtros aplicados.
- c. En la columna **Aplicaciones**, active las casillas de verificación de las aplicaciones para las que desea crear reglas de acceso a archivos cifrados.
- d. En la lista desplegable **Regla para aplicaciones**, seleccione la regla que determinará el acceso de las aplicaciones a los archivos cifrados.

e. En la lista desplegable **Acciones para aplicaciones que se seleccionaron antes**, seleccione la acción que Kaspersky Endpoint Security llevará a cabo en las reglas de acceso a archivos cifrados que se han formado previamente para dichas aplicaciones.

f. Haga clic en **Aceptar**.

La información sobre las reglas de acceso a archivos cifrados para aplicaciones se muestra en la tabla de la pestaña **Reglas para aplicaciones**.

10. Si desea seleccionar manualmente las aplicaciones, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione el elemento **Aplicaciones personalizadas**.

Se abre la ventana **Agregar/editar los nombres de archivos ejecutables de aplicaciones**.

Haga lo siguiente:

a. En el campo de entrada, introduzca el nombre o la lista de nombres de archivos de aplicaciones ejecutables, incluidas sus extensiones.

También puede agregar nombres de archivos ejecutables de aplicaciones de la lista de Kaspersky Security Center haciendo clic en el botón **Agregar de la lista de Kaspersky Security Center**.

b. Si es preciso, en el campo **Descripción**, introduzca una descripción de la lista de aplicaciones.

c. En la lista desplegable **Regla para aplicaciones**, seleccione la regla que determinará el acceso de las aplicaciones a los archivos cifrados.

d. Haga clic en **Aceptar**.

La información sobre las reglas de acceso a archivos cifrados para aplicaciones se muestra en la tabla de la pestaña **Reglas para aplicaciones**.

11. Para guardar los cambios, haga clic en el botón **Aceptar**.

Cifrar archivos creados o modificados por aplicaciones específicas

Puede crear una regla según la cual Kaspersky Endpoint Security cifrará todos los archivos creados o modificados por las aplicaciones especificadas en la regla.

Los archivos que fueron creados o modificados por las aplicaciones especificadas antes de que se aplicara la regla de cifrado no se cifrarán.

Para configurar el cifrado de archivos que se crean o modifican por aplicaciones específicas:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea configurar el descifrado de archivos de unidades de disco locales.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.

5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:

- En el menú contextual de la directiva, seleccione **Propiedades**.
- Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.

6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de archivos y carpetas**.

7. En la lista desplegable **Modo de cifrado**, seleccione el elemento **Reglas predeterminadas**.

Las reglas de cifrado se aplican únicamente en el modo **Mediante reglas**. Después de aplicar reglas de cifrado en el modo **Mediante reglas**, si cambia al modo **Dejar sin modificar**, Kaspersky Endpoint Security ignorará todas las reglas de cifrado. Los archivos que se cifraron con anterioridad permanecerán cifrados.

8. En la parte derecha de la ventana, seleccione la pestaña **Reglas para aplicaciones**.

9. Si desea seleccionar aplicaciones exclusivamente desde la lista de Kaspersky Security Center, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione el elemento **Aplicaciones de la lista de Kaspersky Security Center**.

Se abre la ventana **Agregar aplicaciones de la lista de Kaspersky Security Center**.

Haga lo siguiente:

- a. Especifique los filtros para restringir la lista de aplicaciones de la tabla. Para ello, especifique los valores de los parámetros **Aplicación**, **Proveedor** y **Período agregado**, así como todas las casillas de verificación de la sección **Grupo**.
- b. Haga clic en el botón **Actualizar**.
La tabla muestra las aplicaciones que cumplen los filtros aplicados.
- c. En la columna **Aplicación**, seleccione las casillas de verificación situadas junto a las aplicaciones cuyos archivos creados se deben cifrar.
- d. En la lista desplegable **Regla para aplicaciones**, seleccione **Cifrar todos los archivos creados**.
- e. En la lista desplegable **Acciones para aplicaciones que se seleccionaron antes**, seleccione la acción que Kaspersky Endpoint Security llevará a cabo en las reglas de cifrado de archivos que se han creado previamente para las aplicaciones mencionadas.
- f. Haga clic en **Aceptar**.

La información sobre la regla de cifrado para archivos creados o modificados por las aplicaciones seleccionadas aparece en la tabla de la pestaña **Reglas para aplicaciones**.

10. Si desea seleccionar manualmente las aplicaciones, haga clic en el botón **Agregar** y, en la lista desplegable, seleccione el elemento **Aplicaciones personalizadas**.

Se abre la ventana **Agregar/editar los nombres de archivos ejecutables de aplicaciones**.

Haga lo siguiente:

- a. En el campo de entrada, introduzca el nombre o la lista de nombres de archivos de aplicaciones ejecutables, incluidas sus extensiones.

También puede agregar nombres de archivos ejecutables de aplicaciones de la lista de Kaspersky Security Center haciendo clic en el botón **Agregar de la lista de Kaspersky Security Center**.

- b. Si es preciso, en el campo **Descripción**, introduzca una descripción de la lista de aplicaciones.
- c. En la lista desplegable **Regla para aplicaciones**, seleccione **Cifrar todos los archivos creados**.
- d. Haga clic en **Aceptar**.

La información sobre la regla de cifrado para archivos creados o modificados por las aplicaciones seleccionadas aparece en la tabla de la pestaña **Reglas para aplicaciones**.

11. Para guardar los cambios, haga clic en el botón **Aceptar**.

Generación de una regla de descifrado

Para generar una regla de descifrado:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea generar una lista de archivos que se deben descifrar.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de archivos y carpetas**.
7. En la parte derecha de la ventana, seleccione la pestaña **Descifrado**.
8. En la lista desplegable **Modo de cifrado**, seleccione el elemento **Reglas predeterminadas**.
9. En la pestaña **Descifrado**, haga clic en el botón **Agregar** y en la lista desplegable seleccione uno de los elementos siguientes:
 - a. Seleccione el elemento **Carpetas predeterminadas** para agregar archivos desde carpetas de perfiles de usuario locales sugeridos por expertos de Kaspersky a una regla de descifrado.
Se abre la ventana **Seleccionar carpetas predeterminadas**.
 - b. Seleccione el elemento **Carpeta personalizada** para agregar una ruta de la carpeta introducida manualmente a una regla de descifrado.
Se abre la ventana **Agregar carpeta personalizada**.
 - c. Seleccione el elemento **Archivos por extensión** para agregar extensiones de archivo a una regla de descifrado. Kaspersky Endpoint Security no cifra los archivos de todas las unidades locales del equipo que tienen las extensiones especificadas.
Se abre la ventana **Agregar/modificar la lista de extensiones de archivo**.

d. Seleccione el elemento **Archivos por grupos de extensiones** para agregar grupos de extensiones de archivo a una regla de descifrado. Kaspersky Endpoint Security no cifra archivos cuyas extensiones se incluyen en los grupos de extensiones de todas las unidades de disco locales de los equipos.

Se abre la ventana **Seleccionar grupos de extensiones de archivos**.

10. Para guardar los cambios, en la ventana **Propiedades: <Nombre de directiva>**, haga clic en **Aceptar**.

11. Aplique la directiva.

Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

Si un mismo archivo se ha agregado a la regla de cifrado y a la de descifrado, Kaspersky Endpoint Security no cifra este archivo si está descifrado y descifra el archivo si está cifrado.

Descifrado de archivos de las unidades del equipo local

Para descifrar los archivos de las unidades locales:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea configurar el descifrado de archivos de unidades de disco locales.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de archivos y carpetas**.
7. En la parte derecha de la ventana, seleccione la pestaña **Cifrado**.
8. Elimine los archivos y las carpetas que desea descifrar de la lista de cifrado. Para ello, seleccione los archivos y el elemento **Eliminar regla y descifrar archivos** del menú contextual del botón **Eliminar**.

Puede eliminar varios elementos de la lista de cifrado de una vez. Para ello, mientras mantiene presionada la tecla **CTRL**, seleccione los archivos pertinentes haciendo clic con el botón izquierdo del ratón y seleccione el elemento **Eliminar regla y descifrar archivos** del menú contextual del botón **Eliminar**.

Los archivos y las carpetas que se eliminan de la lista de cifrado se agregan automáticamente a la lista de descifrado.

9. [Cree una lista de descifrado de archivos](#).

10. Para guardar los cambios, en la ventana **Propiedades: <Nombre de directiva>**, haga clic en **Aceptar**.

11. Aplique la directiva.

Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

En cuanto se aplique la directiva, Kaspersky Endpoint Security descifra los archivos cifrados que se agregan a la lista de descifrado.

Kaspersky Endpoint Security descifra los archivos cifrados si sus parámetros (ruta del archivo/nombre del archivo/extensión del archivo) cambian para coincidir con los parámetros de los objetos agregados a la lista de descifrado.

Kaspersky Endpoint Security pospone el descifrado de archivos abiertos hasta que se cierren.

Creación de paquetes cifrados

Kaspersky Endpoint Security no comprime los archivos cuando crea un paquete cifrado.

Para crear un paquete cifrado:

1. En un equipo en el que se haya instalado Kaspersky Endpoint Security y se haya activado la funcionalidad de cifrado, utilice a cualquier administrador de archivos para seleccionar los archivos o las carpetas que desea agregar a un paquete cifrado. Haga clic con el botón derecho del ratón para abrir su menú contextual.
2. En el menú contextual, seleccione **Agregar al paquete cifrado**.
Se abre el cuadro de diálogo estándar **Seleccionar la ruta para guardar el paquete cifrado** de Microsoft Windows.
3. En el cuadro de diálogo estándar **Seleccionar la ruta para guardar el paquete cifrado** de Microsoft Windows, seleccione la carpeta de destino de la unidad extraíble donde se debe guardar el paquete cifrado. Haga clic en el botón **Guardar**.
Se abre la ventana **Agregar al paquete cifrado**.
4. En la ventana **Agregar al paquete cifrado**, introduzca y confirme la contraseña.
5. Haga clic en el botón **Crear**.
Se inicia el proceso de creación del paquete cifrado. Cuando el proceso termina, se crea un paquete cifrado autoextraíble y protegido con contraseña en la carpeta de destino de la unidad extraíble seleccionada.

Si cancela la creación de un paquete cifrado, Kaspersky Endpoint Security realiza las siguientes operaciones:

1. Termina los procesos de copia de archivos al paquete y finaliza todas las operaciones de cifrado del paquete en curso, si existe alguna.
2. Elimina todos los archivos temporales que se han generado durante el proceso de creación y cifrado de un paquete, así como el propio archivo del paquete cifrado.
3. Notifica al usuario que se ha forzado la finalización del proceso de creación del paquete cifrado.

Extracción de los paquetes cifrados

Para extraer un paquete cifrado:

1. En cualquier administrador de archivos, seleccione un paquete cifrado. Haga clic para iniciar el Asistente de descompresión.

Se abre la ventana **Introducir contraseña**.

2. Introduzca la contraseña que protege al paquete cifrado.

3. En la ventana **Introducir contraseña**, haga clic en **Aceptar**.

Si se introduce la contraseña correcta, se abre el cuadro de diálogo estándar **Examinar** de Microsoft Windows.

4. En el cuadro de diálogo estándar **Examinar** de Microsoft Windows, seleccione la carpeta de destino en la que descomprimir el archivo cifrado y haga clic en **Aceptar**.

El proceso de extracción del paquete cifrado en la carpeta de destino se inicia.

Si el paquete cifrado se extrajo previamente en la carpeta de destino especificada, los archivos existentes en la carpeta se sobrescribirán con los archivos del paquete cifrado.

Si cancela la extracción de un paquete cifrado, Kaspersky Endpoint Security realiza las siguientes operaciones:

1. Detiene el proceso de descifrado de paquetes y finaliza todas las operaciones de copia de archivos del paquete cifrado, en caso de que dichas operaciones estén en curso.
2. Elimina todos los archivos temporales creados en el transcurso del descifrado y la extracción del paquete cifrado, así como todos los archivos que ya se han copiado desde el paquete cifrado en la carpeta de destino.
3. Notifica al usuario que se ha forzado la finalización del proceso de extracción del paquete cifrado.

Cifrado de unidades extraíbles

El cifrado de unidades extraíbles está disponible si Kaspersky Endpoint Security se instala en un equipo con Microsoft Windows para estaciones de trabajo. El cifrado de unidades extraíbles no está disponible si Kaspersky Endpoint Security se instala en un equipo con [Microsoft Windows para servidores de archivos](#).

Esta sección contiene información sobre el cifrado de unidades extraíbles e instrucciones para configurar y realizar el cifrado de unidades extraíbles con Kaspersky Endpoint Security y el complemento de administración de Kaspersky Endpoint Security.

Iniciar el cifrado de unidades extraíbles

Para cifrar unidades extraíbles:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea configurar el cifrado de unidades extraíbles.

3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de unidades extraíbles**.
7. En la lista desplegable **Modo de cifrado**, seleccione la acción predeterminada que Kaspersky Endpoint Security debe realizar en todas las unidades extraíbles que estén conectadas a los equipos del grupo de administración seleccionado:
 - **Cifrar la unidad extraíble completa**. Si se selecciona este elemento, al aplicar la directiva de Kaspersky Security Center con la configuración de cifrado de unidades extraíbles especificada, Kaspersky Endpoint Security cifra el contenido de unidades extraíbles sector por sector. Como resultado, la aplicación cifra no solo los archivos almacenados en las unidades extraíbles, sino también los sistemas de archivos de las unidades extraíbles, incluidos los nombres de archivo y estructuras de carpetas. Kaspersky Endpoint Security no vuelve a cifrar las unidades extraíbles que ya se han cifrado anteriormente.

La funcionalidad de cifrado de discos duros de Kaspersky Endpoint Security permite este escenario de cifrado.

- **Cifrar todos los archivos** Si se selecciona este elemento, cuando se aplique la directiva de Kaspersky Security Center con la configuración especificada de cifrado para unidades extraíbles, Kaspersky Endpoint Security cifrará todos los archivos almacenados en las unidades extraíbles. Kaspersky Endpoint Security no cifra los archivos ya cifrados. La aplicación no cifra los sistemas de archivos de las unidades extraíbles, incluidos los nombres de los archivos cifrados y las estructuras de carpetas.
- **Cifrar solo archivos nuevos**. Si se selecciona este elemento, cuando se aplique la directiva de Kaspersky Security Center con la configuración especificada de cifrado para unidades extraíbles, Kaspersky Endpoint Security cifrará solamente los archivos que se han agregado a las unidades extraíbles o se almacenaron en ellas y se han modificado con posterioridad a la última aplicación de la directiva de Kaspersky Security Center.
- **Descifrar la unidad extraíble completa**. Si se selecciona este elemento, cuando se aplique la directiva de Kaspersky Security Center con la configuración de cifrado de unidades extraíbles especificada, Kaspersky Endpoint Security descifrá todos los archivos cifrados que se hayan almacenado en las unidades extraíbles, así como los sistemas de archivos de las unidades extraíbles si estos se hubieran cifrado previamente.

La funcionalidad de cifrado de archivos y la funcionalidad de cifrado de discos duros de Kaspersky Endpoint Security hacen posible este escenario de cifrado.

- **Dejar sin modificar**. Si se selecciona este elemento, cuando se aplique la directiva de Kaspersky Security Center con la configuración especificada de cifrado para unidades extraíbles, Kaspersky Endpoint Security no cifrará ni descifrá los archivos de las unidades extraíbles.
8. [Cree](#) reglas de cifrado de los archivos de las unidades extraíbles cuyo contenido desea cifrar.

9. Aplique la directiva.

Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

Una vez que se aplica la directiva, cuando el usuario conecta una unidad extraíble o si la unidad extraíble ya está conectada, Kaspersky Endpoint Security notifica al usuario que la unidad extraíble está sujeta a una regla de cifrado por la cual se cifran los datos almacenados dicha unidad.

Si se especifica la regla *Dejar sin modificar* para el cifrado de los datos de una unidad extraíble, la aplicación no muestra al usuario ninguna notificación.

La aplicación advierte al usuario de que el proceso de cifrado puede tardar un tiempo.

La aplicación solicita al usuario la confirmación de la operación de cifrado y realiza las siguientes acciones:

- Cifra los datos de acuerdo con la configuración de la directiva, si el usuario consiente el cifrado.
- Mantiene los datos descifrados si el usuario rechaza el cifrado y restringe el acceso a los archivos de la unidad extraíble a solo lectura.
- Mantiene los datos descifrados si el usuario ignora la solicitud de cifrado, restringe el acceso a los archivos de la unidad extraíble a solo lectura y vuelve a solicitar al usuario la confirmación del cifrado de datos la próxima vez que se aplique la directiva de Kaspersky Security Center o que se conecte una unidad extraíble.

La directiva de Kaspersky Security Center que incluye la configuración de cifrado de datos de unidades extraíbles predefinida se crea para un grupo específico de equipos gestionados. Por lo tanto, el resultado del cifrado de datos de unidades extraíbles depende del equipo al cual está conectada la unidad extraíble.

Si el usuario inicia la extracción segura de una unidad extraíble durante el cifrado de datos, Kaspersky Endpoint Security interrumpe el proceso de cifrado de datos y permite la extracción de la unidad extraíble antes de que el proceso de cifrado haya finalizado.

Si el proceso de cifrado de una unidad extraíble falla, puede ver el informe **Cifrado de datos** en la interfaz de Kaspersky Endpoint Security. Es posible que otra aplicación bloquee el acceso a los archivos. En tal caso, pruebe a desconectar la unidad extraíble del equipo y volver a conectarla.

Agregar una regla de cifrado para unidades extraíbles

Para agregar una regla de cifrado de unidades extraíbles:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el cual desea agregar reglas de cifrado de unidades extraíbles.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:

- En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de unidades extraíbles**.
7. Haga clic en el botón **Agregar** con el botón principal del ratón y, en la lista desplegable, seleccione uno de los elementos siguientes:
- Si desea agregar reglas de cifrado para las unidades extraíbles que están en la lista de dispositivos de confianza del componente Control de dispositivos, seleccione **De una lista de dispositivos de confianza de esta directiva**.
Se abre la ventana **Agregar dispositivos de la lista de dispositivos de confianza**.
 - Si desea agregar reglas de cifrado para las unidades extraíbles que están en la lista de Kaspersky Security Center, seleccione **De la lista de dispositivos de Kaspersky Security Center**.
Se abre la ventana **Agregar dispositivos de la lista de Kaspersky Security Center**.
8. Si seleccionó **De la lista de dispositivos de Kaspersky Security Center** durante el paso anterior, especifique los filtros para mostrar dispositivos en la tabla. Para ello:
- a. Especifique los valores de los parámetros siguientes: **Mostrar dispositivos en la tabla para la que se ha definido lo siguiente, Tipo de dispositivo, Nombre, Equipo y Cifrado de disco de Kaspersky**.
 - b. Haga clic en el botón **Actualizar**.
9. En la columna **Tipo de dispositivo**, active las casillas de verificación de los nombres de las unidades extraíbles para las cuales desea crear reglas de cifrado.
10. En la lista desplegable **Modo de cifrado para dispositivos seleccionados**, seleccione la acción que Kaspersky Endpoint Security debe realizar en los archivos almacenados en las unidades extraíbles seleccionadas.
11. Seleccione la casilla de verificación **Modo portátil** si desea que Kaspersky Endpoint Security prepare las unidades extraíbles antes del cifrado, permitiendo, así, utilizar los archivos cifrados que contienen en modo portátil.
El modo portátil le permite utilizar los archivos cifrados almacenados en las unidades extraíbles conectadas a los equipos [que no disponen de la funcionalidad de cifrado](#).
12. Seleccione la casilla de verificación **Cifrar solo el espacio de la unidad utilizado** si desea que Kaspersky Endpoint Security cifre solo esos sectores del disco que están ocupados por archivos.
Si va a aplicar cifrado a una unidad de disco que está ya en uso, se recomienda que cifre la unidad de disco completa. Esto garantiza que se protegen todos los datos, incluso los datos eliminados que todavía podrían contener información recuperable. La función **Cifrar solo el espacio de la unidad utilizado** se recomienda para las unidades nuevas que no se han utilizado anteriormente.
- Si un dispositivo se cifró anteriormente mediante la función **Cifrar solo el espacio de la unidad utilizado**, después de aplicar una directiva en el modo **Cifrar toda la unidad extraíble**, los sectores que aún no están ocupados por archivos no se cifrarán.
13. En la lista desplegable **Acciones para dispositivos que se seleccionaron antes**, seleccione la acción que realizará Kaspersky Endpoint Security conforme a las reglas de cifrado definidas previamente para las unidades extraíbles:

- Si desea que la regla de cifrado creada anteriormente para la unidad extraíble no sufra modificaciones, seleccione **Ignorar**.
- Si desea que una regla de cifrado creada anteriormente para una unidad de eliminación sea reemplazada por la nueva regla, seleccione **Actualizar**.

14. Haga clic en **Aceptar**.

En la tabla **Reglas personalizadas** aparecen las líneas que contienen los parámetros de las reglas de cifrado.

15. Para guardar los cambios, haga clic en el botón **Aceptar**.

Las reglas de cifrado de unidades extraíbles agregadas se aplican a las unidades extraíbles conectadas a cualquier equipo controlado por la directiva modificada de Kaspersky Security Center.

Editar una regla de cifrado para unidades extraíbles

Para modificar una regla de cifrado de una unidad extraíble:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el cual desea editar una regla de cifrado de unidades extraíbles.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de unidades extraíbles**.
7. En la lista de unidades extraíbles para las cuales se han configurado reglas de cifrado, seleccione la entrada correspondiente a la unidad extraíble pertinente.
8. Haga clic en el botón **Establecer una regla** para modificar la regla de cifrado de la unidad extraíble seleccionada.

Se abre el menú contextual del botón **Establecer una regla**.
9. En el menú contextual del botón **Establecer una regla**, seleccione la acción que Kaspersky Endpoint Security debe realizar en los archivos almacenados en la unidad extraíble seleccionada.
10. Para guardar los cambios, haga clic en el botón **Aceptar**.

Las reglas de cifrado de unidades extraíbles modificadas se aplican a las unidades extraíbles conectadas a cualquier equipo controlado por la directiva modificada de Kaspersky Security Center.

Activación del modo portátil para acceder a archivos cifrados de unidades extraíbles

Para activar el modo portátil para acceder a archivos cifrados de unidades extraíbles:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea activar el modo portátil con el fin de acceder a archivos cifrados de unidades extraíbles.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de unidades extraíbles**.
7. Active la casilla de verificación **Modo portátil**.

El modo portátil permite cifrar todos los archivos o solo los nuevos.

8. Haga clic en **Aceptar**.
9. Aplique la directiva.

Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.
10. Conecte el disco extraíble a un dispositivo en el cual se aplicó la directiva de Kaspersky Security Center.
11. Confirme la operación de cifrado del disco extraíble.

Esto abre una ventana en la cual puede crear una contraseña para el [Gestor de archivos portátiles](#).
12. Especifique una contraseña que cumpla con los requisitos de resistencia y confírmela.
13. Haga clic en **Aceptar**.

Kaspersky Endpoint Security cifra archivos de discos extraíbles según las reglas de cifrado definidas en la directiva de Kaspersky Security Center. El Gestor de archivos portátiles utilizado para trabajar con archivos cifrados también se escribirá en el disco extraíble.

Una vez que active el modo portátil, puede acceder a los archivos cifrados de las unidades extraíbles conectadas al equipo sin la necesidad de disponer de la funcionalidad de cifrado.

Descifrado de unidades extraíbles

Para descifrar unidades extraíbles:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea configurar el descifrado de unidades extraíbles.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de unidades extraíbles**.
7. Si desea descifrar todos los archivos cifrados almacenados en las unidades extraíbles, en la lista desplegable **Modo de cifrado**, seleccione **Descifrar toda la unidad extraíble**.
8. Para descifrar los datos que se almacenan en unidades extraíbles individuales, modifique las reglas de cifrado de las unidades extraíbles cuyos datos desea descifrar. Para ello:
 - a. En la lista de unidades extraíbles para las cuales se han configurado reglas de cifrado, seleccione la entrada correspondiente a la unidad extraíble pertinente.
 - b. Haga clic en el botón **Establecer una regla** para modificar la regla de cifrado de la unidad extraíble seleccionada.

Se abre el menú contextual del botón **Establecer una regla**.
 - c. Seleccione el elemento **Descifrar todos los archivos** del menú contextual del botón **Establecer una regla**.
9. Para guardar los cambios, haga clic en el botón **Aceptar**.
10. Aplique la directiva.

Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

Después de que se haya aplicado la directiva, cuando el usuario conecta una unidad extraíble o si una unidad extraíble está conectada ya, Kaspersky Endpoint Security notifica al usuario que la unidad extraíble está conforme a una regla de cifrado por el que los archivos cifrados almacenados en la unidad extraíble, así como el sistema del archivo de la unidad extraíble (si se cifra) sean descifrados. La aplicación advierte al usuario de que el proceso de descifrado puede tardar un tiempo.

La directiva de Kaspersky Security Center que incluye la configuración de cifrado de datos de unidades extraíbles predefinida se crea para un grupo específico de equipos gestionados. Por lo tanto, el resultado del descifrado de los datos en las unidades extraíbles depende del equipo con el cual la unidad extraíble está conectada.

Si el usuario inicia la extracción segura de una unidad extraíble durante el descifrado de datos, Kaspersky Endpoint Security interrumpe el proceso de descifrado de datos y permite la extracción de la unidad extraíble antes de que la operación de descifrado haya finalizado.

Si el proceso de descifrado de una unidad extraíble falla, puede ver el informe **Cifrado de datos** en la interfaz de Kaspersky Endpoint Security. Es posible que otra aplicación bloquee el acceso a los archivos. En tal caso, pruebe a desconectar la unidad extraíble del equipo y volver a conectarla.

Cifrado de discos duros

Si Kaspersky Endpoint Security se instala en un equipo en el que se ejecuta Microsoft Windows para estaciones de trabajo, las tecnologías de Cifrado de unidad BitLocker y Cifrado de disco de Kaspersky están disponibles. Si Kaspersky Endpoint Security se instala en un equipo en el que se ejecuta [Microsoft Windows para servidores de archivos](#), solo está disponible la tecnología Cifrado de unidad BitLocker.

Esta sección contiene información sobre el cifrado de discos duros e instrucciones para configurar y realizar el cifrado de estos con Kaspersky Endpoint Security y el complemento de consola de Kaspersky Endpoint Security.

Acerca del cifrado de discos duros

Antes de empezar el cifrado del disco duro, la aplicación ejecuta una serie de comprobaciones para determinar si el dispositivo se puede cifrar. Esto incluye la comprobación del disco duro del sistema para averiguar si es compatible con Agente de autenticación y los componentes de cifrado de BitLocker. Para comprobar la compatibilidad, el equipo se debe reiniciar. Tras el reinicio, la aplicación llevará a cabo todas las comprobaciones necesarias automáticamente. Si se supera la comprobación de compatibilidad, el cifrado del disco duro comenzará después de que el sistema operativo se haya cargado y la aplicación se haya iniciado. Si se determina que el disco duro del sistema no es compatible con Agente de autenticación o con los componentes de cifrado de BitLocker, se deberá reiniciar el equipo pulsando el botón físico de reinicio. Kaspersky Endpoint Security registra información sobre la incompatibilidad. En función de esta información, la aplicación no comenzará el cifrado de discos duros cuando arranque el sistema operativo. La información sobre este evento se registra en informes de Kaspersky Security Center.

Si la configuración de hardware del equipo ha cambiado, se deberá eliminar la información de incompatibilidad registrada por la aplicación durante la comprobación anterior para averiguar la compatibilidad del disco duro del sistema con el Agente de autenticación y los componentes de cifrado de BitLocker. Para ello, escriba `avp pbatestreset` en la línea de comandos antes del cifrado del disco duro. Si el sistema operativo no se carga después de que se haya comprobado la compatibilidad del disco duro del sistema con Agente de autenticación, [debe quitar los objetos y los datos que permanecen tras la operación de prueba del Agente de autenticación](#) con la Utilidad de restauración. A continuación, inicie Kaspersky Endpoint Security y vuelva a ejecutar el comando `avp pbatestreset`.

Cuando comience el cifrado del disco duro, Kaspersky Endpoint Security cifra todos los datos escritos en los discos duros.

Si el usuario apaga o reinicia el equipo durante la tarea de descifrado del disco duro, Agente de autenticación se carga antes del siguiente inicio del sistema operativo. Kaspersky Endpoint Security reanuda el cifrado de discos duros después de la autenticación correcta en el agente de autenticación y del arranque del sistema operativo.

Si el sistema operativo cambia al modo de hibernación mientras cifra discos duros, Agente de autenticación se carga cuando el sistema operativo vuelve al modo normal. Kaspersky Endpoint Security reanuda el cifrado de discos duros después de la autenticación correcta en el agente de autenticación y del arranque del sistema operativo.

Si el sistema operativo entra en modo de suspensión durante el cifrado de discos duros, Kaspersky Endpoint Security reanudará el proceso cuando el sistema operativo salga del modo de suspensión sin cargar el Agente de autenticación.

La autenticación de usuario en Agente de autenticación se puede realizar de dos maneras:

- Introduzca el nombre y la contraseña de la cuenta del Agente de autenticación creada por el administrador de la red de área local con las herramientas de Kaspersky Security Center.
- Introduzca la contraseña de un token o una tarjeta inteligente conectados al equipo.

El agente de autenticación admite las distribuciones del teclado para los siguientes idiomas:

- Inglés (Reino Unido)
- Inglés (EE. UU.)
- Árabe (Argelia, Marruecos, Túnez; diseño AZERTY)
- Español (América Latina)
- Italiano
- Alemán (Alemania y Austria)
- Alemán (Suiza)
- Portugués (Brasil; diseño ABNT2)
- Ruso (para teclados IBM de 105 teclas o teclados Windows con el diseño QWERTY)
- Turco (diseño QWERTY)
- Francés (Francia)
- Francés (Suiza)
- Francés (Bélgica, diseño AZERTY)
- Japonés (para teclados de 106 teclas con el diseño QWERTY)

Hay una distribución del teclado disponible en el Agente de autenticación si esta se ha agregado en el idioma y con la configuración regional estándar del sistema operativo, y aparece disponible en la pantalla de bienvenida de Microsoft Windows.

Si el nombre de la cuenta del Agente de autenticación contiene símbolos que no pueden introducirse mediante las distribuciones del teclado disponibles en el Agente de autenticación, solo es posible acceder a los discos duros cifrados después de su restauración mediante la [Utilidad de restauración](#) o después de que [se restauren el nombre de la cuenta y la contraseña del Agente de autenticación](#).

Kaspersky Endpoint Security admite los tókenes, los lectores de tarjeta inteligente y las tarjetas inteligentes siguientes:

- SafeNet eToken PRO 64 K (4.2b) (USB)
- SafeNet eToken PRO 72 K Java (USB)
- SafeNet eToken PRO 72 K Java (tarjeta inteligente)
- SafeNet eToken 4100 72K Java (tarjeta inteligente)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB)
- Rutoken EDS (Flash)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (tarjeta inteligente)
- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (lector)
- Gemalto IDPrime .NET 511

Cifrado de discos duros mediante la tecnología Cifrado de disco de Kaspersky

Antes de llevar a cabo el cifrado de discos duros en un equipo, se recomienda que se asegure de que el equipo no está infectado. Para ello, ejecute [la tarea Análisis completo o Análisis de áreas críticas](#). El cifrado del disco duro de un equipo infectado por un rootkit puede hacer que deje de funcionar.

Para cifrar discos duros mediante la tecnología Cifrado de disco de Kaspersky:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea configurar el cifrado de discos duros.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.

5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:

- En el menú contextual de la directiva, seleccione **Propiedades**.
- Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.

6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de discos duros**.

7. En la lista desplegable **Tecnología de cifrado**, seleccione la opción **Cifrado de disco de Kaspersky**.

La tecnología Cifrado de disco de Kaspersky no se puede utilizar si el equipo cuenta con discos duros cifrados por BitLocker.

8. En la lista desplegable **Modo de cifrado**, seleccione **Cifrar todos los discos duros**.

Si tiene que excluir algunos de los discos duros del cifrado, [cree una lista de estos discos duros](#).

9. Seleccione uno de los siguientes métodos de cifrado:

- Si desea aplicar el cifrado solo a los sectores del disco duro que están ocupados por archivos, seleccione la casilla de verificación **Cifrar solo el espacio de la unidad utilizado**.

Si va a aplicar cifrado a una unidad de disco que está ya en uso, se recomienda que cifre la unidad de disco completa. Esto garantiza que se protegen todos los datos, incluso los datos eliminados que todavía podrían contener información recuperable. La función **Cifrar solo el espacio de la unidad utilizado** se recomienda para las unidades nuevas que no se han utilizado anteriormente.

- Si desea aplicar el cifrado al disco duro completo, desactive la casilla de verificación **Cifrar solo el espacio de la unidad utilizado**.

Esta función solo es aplicable a dispositivos no cifrados. Si un dispositivo se cifró anteriormente mediante la función **Cifrar solo el espacio de la unidad utilizado**, después de aplicar una directiva en el modo **Cifrar todos los discos duros**, los sectores que aún no están ocupados por archivos no se cifrarán.

10. Para guardar los cambios, haga clic en el botón **Aceptar**.

11. Aplique la directiva.

Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

Cifrar discos duros mediante la tecnología Cifrado de unidad BitLocker

Antes de llevar a cabo el cifrado de discos duros en un equipo, se recomienda que se asegure de que el equipo no está infectado. Para ello, ejecute [la tarea Análisis completo o Análisis de áreas críticas](#). El cifrado del disco duro de un equipo infectado por un rootkit puede hacer que deje de funcionar.

El uso de la tecnología de Cifrado de unidad BitLocker en equipos con un sistema operativo de servidor puede requerir la instalación del componente **Cifrado de unidad BitLocker** mediante el asistente para agregar roles y componentes.

Para cifrar discos duros con la tecnología Cifrado de unidad BitLocker:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea configurar el cifrado de discos duros.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de discos duros**.
7. En la lista desplegable **Tecnología de cifrado**, seleccione la opción **Cifrado de unidad BitLocker**.
8. En la lista desplegable **Modo de cifrado**, seleccione la opción **Cifrar todos los discos duros**.
9. Si desea utilizar un teclado de pantalla táctil para introducir la información en un entorno anterior al arranque, seleccione la casilla de verificación **Permitir el uso de autenticación que requiera entrada de teclado previa al arranque en tabletas**.

Se recomienda utilizar este ajuste solo para dispositivos que tienen herramientas alternativas para la introducción de datos; por ejemplo, un teclado USB en un entorno anterior al arranque.

10. Seleccione uno de los siguientes tipos de cifrado:
 - Si desea usar el cifrado de hardware, seleccione la casilla de verificación **Utilizar cifrado de hardware**.
 - Si desea usar el cifrado de software, desactive la casilla de verificación **Utilizar cifrado de hardware**.
11. Seleccione uno de los siguientes métodos de cifrado:
 - Si desea aplicar el cifrado solo a los sectores del disco duro que están ocupados por archivos, seleccione la casilla de verificación **Cifrar solo el espacio de la unidad utilizado**.
 - Si desea aplicar el cifrado al disco duro completo, desactive la casilla de verificación **Cifrar solo el espacio de la unidad utilizado**.

Esta función solo es aplicable a dispositivos no cifrados. Si un dispositivo se cifró anteriormente mediante la función **Cifrar solo el espacio de la unidad utilizado**, después de aplicar una directiva en el modo **Cifrar todos los discos duros**, los sectores que aún no están ocupados por archivos no se cifrarán.

12. Seleccione un método para acceder a discos duros que se cifraron con BitLocker.

- Si desea utilizar un [módulo de plataforma segura](#) (TPM) para almacenar claves de cifrado, seleccione la opción **Usar el módulo de plataforma segura (TPM)**.
- Si no está usando un módulo de plataforma segura (TPM) para el cifrado de discos duros, seleccione la opción **Usar contraseña** y especifique el número mínimo de caracteres que debe contener una contraseña en el campo **Longitud mínima de la contraseña**.

La disponibilidad de un Módulo de plataforma segura (TPM) es obligatoria para sistemas operativos Windows 7 y Windows 2008 R2, así como para versiones anteriores.

13. Si seleccionó la opción **Usar el módulo de plataforma segura (TPM)** durante el paso anterior:

- Si desea configurar un código del PIN que se solicitará cuando el usuario intente acceder a una clave de cifrado, seleccione la casilla de verificación **Utilizar PIN** y, en el campo **Longitud mínima de PIN**, especifique el número mínimo de dígitos que debe contener un código PIN.
- Si quisiera acceder a discos duros cifrados sin un módulo de plataforma segura en un equipo en el que se usa una contraseña, seleccione la casilla de verificación **Usar contraseña si el módulo de plataforma segura (TPM) no está disponible** y, en el campo **Longitud mínima de la contraseña**, indique el número mínimo de caracteres que la contraseña debería contener.

En este evento, podrá acceder a las claves de cifrado usando la contraseña proporcionada, como si la casilla de verificación **Usar contraseña** estuviera seleccionada.

Si no se seleccionó la casilla de verificación **Usar contraseña si el módulo de plataforma segura (TPM) no está disponible** y el módulo de plataforma segura no está disponible, no comenzará el cifrado del disco duro.

14. Para guardar los cambios, haga clic en el botón **Aceptar**.

15. Aplique la directiva.

Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

Después de aplicar la directiva en el equipo cliente con Kaspersky Endpoint Security instalado, se realizarán las siguientes consultas:

- Si la directiva de cifrado se aplica a un disco duro del sistema, aparecerá la ventana Código PIN si el módulo de plataforma segura está en uso. De lo contrario, la ventana de solicitud de contraseña aparecerá para la autorización de la precarga.
- Si el sistema operativo del equipo tiene el modo de compatibilidad de estándares de procesamiento de información federales activado, en Windows 8 y posteriores, el sistema operativo mostrará una ventana de solicitud de conexión del dispositivo USB para guardar el archivo de clave de recuperación.

Si no hay acceso a claves de cifrado, el usuario puede solicitar que el administrador de la red local proporcione una [clave de recuperación](#) (siempre que la clave de recuperación no se haya guardado anteriormente en el dispositivo USB o se haya perdido).

Creación de una lista de discos duros excluidos del cifrado

Puede crear una lista de exclusiones de cifrado solo para la tecnología Cifrado de disco de Kaspersky.

Para crear una lista de discos duros excluidos del cifrado:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea crear una lista de discos duros que se deben excluir del cifrado.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de discos duros**.
7. En la lista desplegable **Tecnología de cifrado**, seleccione la opción **Cifrado de disco de Kaspersky**.

Las entradas que corresponden a los discos duros excluidos del cifrado aparecen en la tabla **No cifrar los siguientes discos duros**. Esta tabla estará vacía si no ha creado previamente una lista de discos duros que se deben excluir del cifrado.
8. Para agregar discos duros a la lista de discos duros excluidos del cifrado:
 - a. Haga clic en el botón **Agregar**.

Se abre la ventana **Agregar dispositivos de la lista de Kaspersky Security Center**.
 - b. En la ventana **Agregar dispositivos de la lista de Kaspersky Security Center**, especifique los valores de los siguientes parámetros: **Nombre**, **Equipo**, **Tipo de disco** y **Cifrado de disco de Kaspersky**.
 - c. Haga clic en el botón **Actualizar**.
 - d. En la columna **Nombre**, seleccione las casillas de verificación en las filas de la tabla que corresponden a los discos duros que desea agregar a la lista de discos duros excluidos del cifrado.
 - e. Haga clic en **Aceptar**.

Los discos duros seleccionados aparecen en la tabla **No cifrar los siguientes discos duros**.

9. Si desea eliminar discos duros desde la tabla de exclusiones, seleccione una o varias líneas de la tabla **No cifrar los siguientes discos duros**: y haga clic en el botón **Eliminar**.

Para seleccionar varias líneas en la tabla, mantenga pulsada la tecla **CTRL** mientras las selecciona.

10. Para guardar los cambios, haga clic en el botón **Aceptar**.

Descifrado de discos duros

Puede descifrar discos duros aun si no hay licencia activa que permita el cifrado de datos.

Para descifrar discos duros:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea configurar el descifrado de discos duros.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Cifrado de discos duros**.
7. En la lista desplegable **Tecnología de cifrado**, seleccione la tecnología con la que se cifraron los discos duros.
8. Realice una de las siguientes acciones:
 - En la lista desplegable **Modo de cifrado**, seleccione la opción **Descifrar todos los discos duros** para descifrar todos los discos duros cifrados.
 - [Agregue](#) los discos duros cifrados que desea descifrar a la tabla **No cifrar los siguientes discos duros**.

Esta opción solo está disponible para la tecnología Cifrado de disco de Kaspersky.

9. Para guardar los cambios, haga clic en el botón **Aceptar**.

10. Aplique la directiva.

Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

Si el usuario apaga o reinicia el equipo durante el descifrado de discos duros que fueron cifrados mediante tecnología de cifrado de disco de Kaspersky, el Agente de autenticación se carga antes del siguiente inicio del sistema operativo. Kaspersky Endpoint Security reanuda el descifrado del disco duro después de la autenticación correcta en el agente de autenticación y del arranque del sistema operativo.

Si el sistema operativo cambia al modo de hibernación mientras se cifran discos duros que fueron cifrados mediante la tecnología de cifrado de disco de Kaspersky, el Agente de autenticación se carga cuando el sistema operativo sale del modo de hibernación. Kaspersky Endpoint Security reanuda el descifrado del disco duro después de la autenticación correcta en el agente de autenticación y del arranque del sistema operativo. Después de descifrar el disco duro, no se encontrará disponible el modo de hibernación hasta que se realice un primer reinicio del sistema operativo.

Si el sistema operativo entra en modo de suspensión durante el descifrado del disco duro, Kaspersky Endpoint Security reanudará el descifrado del disco duro cuando el sistema operativo salga del modo de hibernación sin cargar el Agente de autenticación.

Gestionar el Agente de autenticación

Si los discos duros del sistema están cifrados, el Agente de autenticación se carga antes del inicio del sistema operativo. Utilice el Agente de autenticación para completar la autenticación con el fin de obtener acceso a los discos duros cifrados del sistema y cargar el sistema operativo.

Después de que se completa correctamente el procedimiento de autenticación, se carga el sistema operativo. Se repite el proceso de autenticación cada vez que el sistema operativo se reinicia.

En algunos casos, el usuario no podrá autenticarse. Por ejemplo, la autenticación es imposible si el usuario ha olvidado las credenciales de la cuenta del Agente de autenticación, o bien ha olvidado la contraseña del token o la tarjeta inteligente o extraviado uno de estos dispositivos.

Si el usuario ha olvidado las credenciales de la cuenta del Agente de autenticación o la contraseña del token o la tarjeta inteligente, se debe poner en contacto con el administrador de la red de área local corporativa [para recuperarlas](#).

Si un usuario ha perdido un token o una tarjeta inteligente, el administrador debe [agregar el archivo del certificado electrónico del token o la tarjeta inteligente](#) al comando para crear una cuenta del Agente de autenticación. Luego, el usuario debe completar el procedimiento de [restauración de datos de dispositivos cifrados](#).

Utilizar una tarjeta inteligente y un token con el Agente de autenticación

Se puede utilizar una tarjeta inteligente o token para la autenticación cuando se accede a discos duros cifrados. Para ello, debe agregar el archivo del certificado electrónico de una tarjeta inteligente o token al comando para crear una cuenta del Agente de autenticación.

El uso de una tarjeta inteligente o token solo está disponible si los discos duros del equipo se cifraron con el algoritmo de cifrado AES256. Si los discos duros del equipo se cifraron usando el algoritmo de cifrado AES56, no se podrá agregar el archivo del certificado electrónico al comando.

Para agregar el archivo de un certificado electrónico de token o tarjeta inteligente al comando con el fin de crear una cuenta del agente de autenticación, debe guardar primero el archivo usando el software de terceros para gestionar certificados.

El certificado del token o tarjeta inteligente tiene que tener las propiedades siguientes:

- El certificado debe cumplir con el estándar X.509 y el archivo de certificado tiene que tener codificación DER.

Si el certificado electrónico del token o la tarjeta inteligente no cumple este requisito, el complemento de administración no carga el archivo de este certificado en el comando para crear una cuenta del Agente de autenticación y muestra un mensaje de error.

- El parámetro KeyUsage que define el propósito del certificado tiene que tener el valor keyEncipherment o dataEncipherment.

Si el certificado electrónico del token o la tarjeta inteligente no cumple este requisito, el complemento de administración carga el archivo de este certificado en el comando para crear una cuenta del Agente de autenticación y muestra un mensaje de advertencia.

- El certificado contiene una clave RSA con una longitud de al menos 1024 bits.

Si el certificado electrónico del token o la tarjeta inteligente no cumple este requisito, el complemento de administración no carga el archivo de este certificado en el comando para crear una cuenta del Agente de autenticación y muestra un mensaje de error.

Editar los mensajes de ayuda del Agente de autenticación

Antes de editar mensajes de ayuda del Agente de autenticación, revise la [lista de caracteres admitidos en un entorno anterior al arranque](#).

Para editar los mensajes de ayuda del Agente de autenticación:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración para el que desea editar los mensajes de ayuda del Agente de autenticación.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Configuración común de cifrado**.
7. En la sección **Plantillas**, haga clic en el botón **Ayuda**.
Esto abre la ventana **Mensajes de ayuda del Agente de autenticación**.
8. Haga lo siguiente:
 - Seleccione la pestaña **Autenticación** para editar el texto de ayuda que se muestra en la ventana Agente de autenticación cuando se introducen las credenciales de la cuenta.
 - Seleccione la pestaña **Cambiar la contraseña** para editar el texto de ayuda que se muestra en la ventana del Agente de autenticación cuando se cambia la contraseña de la cuenta del Agente de autenticación.
 - Seleccione la pestaña **Recuperar la contraseña** para modificar el texto de ayuda que se muestra en la ventana del Agente de autenticación cuando se recupera la contraseña de la cuenta del Agente de autenticación.

9. Modifique los mensajes de la ayuda.

Si desea restaurar el texto original, haga clic en el botón **Predeterminado**.

10. Haga clic en **Aceptar**.

11. Para guardar los cambios, en la ventana **Propiedades: <Nombre de directiva>**, haga clic en **Aceptar**.

Compatibilidad limitada con los caracteres de los mensajes de ayuda del Agente de autenticación

En un entorno anterior al arranque, se admiten los siguientes caracteres de Unicode:

- Alfabeto latino básico (0000 - 007F)
- Caracteres de Latino-1 adicionales (0080 - 00FF)
- Latino-A ampliado (0100 - 017F)
- Latino-A ampliado (0180 - 024F)
- Caracteres de ID ampliados no combinados (02B0 - 02FF)
- Marcas diacríticas combinadas (0300 - 036F)
- Alfabetos griego y copto (0370 - 03FF)
- Alfabeto cirílico (0400 - 04FF)
- Hebreo (0590 - 05FF)
- Script árabe (0600 - 06FF)
- Latino ampliado adicional (1E00 - 1EFF)
- Signos de puntuación (2000 - 206F)
- Símbolos de divisa (20A0 - 20CF)
- Símbolos parecidos a una letra (2100 - 214F)
- Cifras geométricas (25A0 - 25FF)
- Formularios de presentación de alfabeto árabe B (FE70 - FEFF)

Los caracteres que no se especifican en esta lista no se admiten en un entorno anterior al arranque. No se recomienda usar tales caracteres en mensajes de ayuda del Agente de autenticación.

Seleccionar el nivel de rastreo del Agente de autenticación

La aplicación registra información de servicio sobre el funcionamiento del Agente de autenticación e información sobre las operaciones de usuario con el Agente de autenticación en el archivo de rastreo. El archivo de rastreo del Agente de autenticación puede resultar muy útil cuando se tiene que [restaurar datos en discos duros cifrados](#).

Para seleccionar el nivel de rastreo del Agente de autenticación:

1. En cuanto se inicie un equipo con discos duros cifrados, pulse el botón **F3** para llamar a una ventana y configurar los ajustes del Agente de autenticación.
2. Seleccione el nivel de rastreo en la ventana de configuración del Agente de autenticación:
 - **Desactivar el registro de depuración (predeterminado).** Si esta opción se selecciona, la aplicación no registra la información de eventos del Agente de autenticación en el archivo de rastreo.
 - **Activar el registro de depuración.** Si se selecciona esta opción, la aplicación registra información sobre el funcionamiento del agente de autenticación y las operaciones de usuario realizadas con el Agente de autenticación en el archivo de rastreo.
 - **Activar el registro detallado.** Si se selecciona esta opción, la aplicación registra información detallada sobre el funcionamiento del Agente de autenticación y las operaciones de usuario realizadas con el Agente de autenticación en el archivo de rastreo.

El nivel de detalle de las entradas de esta opción es superior en comparación con el nivel de la opción **Activar el registro de depuración**. Un nivel elevado de detalle de las entradas puede ralentizar el inicio del Agente de autenticación y del sistema operativo.

- **Activar registro de depuración y seleccionar puerto serie.** Si se selecciona esta opción, la aplicación registra información sobre el funcionamiento del Agente de autenticación y las operaciones de usuario realizadas con el Agente de autenticación en el archivo de rastreo y las transmite a través del puerto COM. Si un equipo con discos duros cifrados está conectado a otro equipo a través del puerto COM, los eventos del Agente de autenticación se pueden examinar desde este otro equipo.
- **Activar el registro de depuración detallado y seleccionar puerto serie.** Si se selecciona esta opción, la aplicación incluye entradas detalladas sobre el funcionamiento del Agente de autenticación y las operaciones de usuario realizadas con el Agente de autenticación en el archivo de rastreo, y las transmite a través del puerto COM.

El nivel de detalle de las entradas de esta opción es superior en comparación con el nivel de la opción **Activar registro de depuración y seleccionar puerto serie**. Un nivel elevado de detalle de las entradas puede ralentizar el inicio del Agente de autenticación y del sistema operativo.

Los datos se registran en el archivo de rastreo del Agente de autenticación si hay discos duros cifrados en el equipo o durante el cifrado de discos duros.

El archivo de rastreo del Agente de autenticación no se envía a Kaspersky a diferencia de otros archivos de rastreo de la aplicación. Si fuera necesario, el administrador del sistema puede enviar manualmente el archivo de rastreo del Agente de autenticación a Kaspersky para su análisis.

Administración de cuentas del Agente de autenticación

Las siguientes herramientas de Kaspersky Security Center están disponibles para administrar las cuentas del Agente de autenticación:

- Tarea de grupo para gestionar cuentas del Agente de autenticación. Esta tarea le permite administrar las cuentas del Agente de autenticación de un grupo de equipos cliente.
- Tarea local **Cifrado (administración de cuentas)**. Esta tarea le permite administrar las cuentas del Agente de autenticación de equipos cliente particulares.

Para configurar los ajustes de la tarea de administración de cuentas del Agente de autenticación:

1. Cree ([Creación de una tarea local](#), [Creación de una tarea de grupos](#)) una tarea de administración de cuentas del Agente de autenticación.
2. [Abra](#) la sección **Configuración** de la ventana **Propiedades**: <nombre de la tarea de administración de la cuenta del Agente de autenticación>.
3. [Agregue comandos para crear cuentas del Agente de autenticación](#).
4. [Agregue comandos para modificar las cuentas del Agente de autenticación](#).
5. [Agregue comandos para eliminar cuentas de usuario del Agente de autenticación](#).
6. En caso de ser necesario, modifique los comandos agregados para administrar las cuentas del Agente de autenticación. Para ello, seleccione un comando de la tabla **Comandos para gestionar las cuentas del agente de autenticación** y haga clic en el botón **Editar**.
7. En caso de ser necesario, elimine los comandos agregados para administrar las cuentas del Agente de autenticación. Para ello, seleccione uno o varios comandos de la tabla **Comandos para gestionar las cuentas del Agente de autenticación** y haga clic en el botón **Eliminar**.

Para seleccionar varias líneas en la tabla, mantenga pulsada la tecla **CTRL** mientras las selecciona.

8. Para guardar los cambios, haga clic en **Aceptar** en la ventana de propiedades de la tarea.
9. [Ejecute la tarea](#).

Se ejecutan los comandos de gestión de la cuenta del Agente de autenticación que se han agregado a la tarea.

Adición de un comando para crear una cuenta del Agente de autenticación

Para agregar un comando para crear una cuenta del Agente de autenticación:

1. [Abra](#) la sección **Configuración** de la ventana **Propiedades**: <nombre de la tarea de administración de la cuenta del Agente de autenticación>.
2. Haga clic en el botón **Agregar** y, en la lista desplegable, seleccione **Comando de adición de cuentas**.
Se abre la ventana **Agregar cuenta de usuario**.
3. En el campo **Agregar cuenta de usuario** de la ventana **Cuenta de Windows**, especifique el nombre de la cuenta de usuario de Microsoft Windows en el que se basará la cuenta del Agente de autenticación que se creará.
Para ello, introduzca el nombre de la cuenta manualmente o haga clic en el botón **Seleccionar**.
4. Si ha introducido el nombre de una cuenta de Microsoft Windows manualmente, haga clic en el botón **Autorizar** para establecer el identificador de seguridad (SID) de la cuenta.

Si prefiere no establecer el identificador de seguridad (SID) por medio del botón **Autorizar**, se establecerá el SID en el momento en el que se realice la tarea en el equipo.

Establecer el SID de la cuenta de usuario de Microsoft Windows cuando se agrega un comando de creación de cuentas del Agente de autenticación resulta muy práctico para asegurarse de que el nombre de la cuenta de usuario de Microsoft Windows que se ha introducido manualmente es correcto. La tarea de administración de la cuenta de usuario del Agente de autenticación finaliza con un error si la cuenta de usuario de Microsoft Windows que se ha introducido no existe, si esta pertenece a un dominio no confiable o si no existe en el equipo para el cual se modifica la tarea local **Cifrado (gestión de cuentas)**.

5. Active la casilla de verificación **Cambiar la cuenta de usuario actual** para tener una cuenta cuyo nombre sea idéntico al de la cuenta del agente de autenticación que se ha creado previamente y que se reemplazará por la cuenta que se está creando.

Este paso está disponible cuando agrega un comando de creación de cuentas del Agente de autenticación en las propiedades de una tarea de grupo para administrar las cuentas del Agente de autenticación. Este paso no está disponible si va a agregar un comando de creación de cuentas del Agente de autenticación en las propiedades de una tarea local **Cifrado (administración de cuentas)**.

6. En el campo **Nombre de usuario**, introduzca el nombre de la cuenta del Agente de autenticación que debe introducirse durante el proceso de autenticación para acceder los discos duros cifrados.
7. Seleccione la casilla de verificación **Autorizar la autenticación basada en contraseña** si desea que la aplicación solicite al usuario que introduzca la contraseña de la cuenta del Agente de autenticación durante la autenticación para acceder a los discos duros cifrados.
8. Si seleccionó la casilla de verificación **Autorizar la autenticación basada en contraseña** durante el paso anterior:
 - a. En el campo **Contraseña**, introduzca la contraseña de la cuenta del Agente de autenticación que debe introducirse durante el proceso de autenticación para acceder los discos duros cifrados.
 - b. En el campo **Confirmar contraseña**, confirme la contraseña de la cuenta del Agente de autenticación introducida en el paso anterior.
 - c. Realice una de las siguientes acciones:
 - Active la opción **Cambiar la contraseña en la primera autenticación** si desea que la aplicación solicite el cambio de contraseña al usuario que se autentica con la cuenta especificada en el comando por primera vez.
 - Si no, seleccione la opción **No solicitar el cambio de contraseña**.
9. Seleccione la casilla de verificación **Autorizar la autenticación basada en certificado** si desea que la aplicación solicite al usuario que se conecte a un token o a tarjeta inteligente conectada al equipo durante la autenticación para acceder a los discos duros cifrados.
10. Si seleccionó la casilla de verificación **Autorizar la autenticación basada en contraseña** durante el paso anterior, haga clic en el botón **Examinar** y seleccione el archivo del certificado electrónico de la tarjeta inteligente o el token en la ventana **Seleccionar el archivo de certificado**.
11. En el campo **Descripción de comandos**, introduzca la información de la cuenta del Agente de autenticación necesaria para administrar el comando.

12. Realice una de las siguientes acciones:

- Seleccione la casilla de verificación **Autorizar autenticación** si desea que la aplicación autorice al usuario que utiliza la cuenta especificada en el comando a acceder al cuadro de diálogo del Agente de autenticación.
- Seleccione la casilla de verificación **Bloquear autenticación** si desea que la aplicación bloquee al usuario que utiliza la cuenta especificada en el comando para que no acceda al cuadro de diálogo del Agente de autenticación.

13. En la ventana **Agregar cuenta de usuario**, haga clic en **Aceptar**.

Agregar un comando de modificación de cuentas del Agente de autenticación

Para agregar un comando con el fin de editar una cuenta del Agente de autenticación:

1. En la sección **Configuración** de la ventana **Propiedades: <nombre de la tarea de administración de las cuentas del Agente de autenticación>**, abra el menú contextual del botón **Agregar** y seleccione el elemento **Comando de modificación de cuentas**.

Se abre la ventana **Modificar cuenta de usuario**.

2. En el campo **Cuenta de Windows** de la ventana **Modificar cuenta de usuario**, especifique el nombre de la cuenta de usuario de Microsoft Windows que se utilizó para crear la cuenta del Agente de autenticación que desea editar. Para ello, introduzca el nombre de la cuenta manualmente o haga clic en el botón **Seleccionar**.
3. Si ha introducido el nombre de una cuenta de usuario de Microsoft Windows manualmente, haga clic en el botón **Autorizar** para establecer el identificador de seguridad (SID) de la cuenta de usuario.

Si prefiere no establecer el identificador de seguridad (SID) por medio del botón **Autorizar**, se establecerá el SID en el momento en el que se realice la tarea en el equipo.

Establecer el SID de la cuenta de usuario de Microsoft Windows cuando se agrega un comando de modificación de cuentas del Agente de autenticación resulta muy práctico para asegurarse de que el nombre de la cuenta de usuario de Microsoft Windows que se ha introducido manualmente es correcta. La tarea de grupo de administración de la cuenta del Agente de autenticación no finaliza de forma correcta si la cuenta de usuario de Microsoft Windows que se ha introducido no existe o pertenece a un dominio no confiable.

4. Active la casilla de verificación **Cambiar el nombre de usuario** e introduzca un nombre de cuenta del Agente de autenticación nuevo si desea que Kaspersky Endpoint Security sustituya el nombre de usuario de todas las cuentas del Agente de autenticación que se hayan creado en función de la cuenta de Microsoft Windows que lleva el nombre que se indica en el campo **Cuenta de Windows** por el nombre introducido en el siguiente campo.
5. Seleccione la casilla de verificación **Modificar la configuración de la autenticación basada en contraseña** para poder editar los ajustes de autenticación basada en contraseña.
6. Seleccione la casilla de verificación **Autorizar la autenticación basada en contraseña** si desea que la aplicación solicite al usuario que introduzca la contraseña de la cuenta del Agente de autenticación durante la autenticación para acceder a los discos duros cifrados.

7. Si seleccionó la casilla de verificación **Autorizar la autenticación basada en contraseña** durante el paso anterior:
 - a. En el campo **Contraseña**, introduzca la nueva contraseña de la cuenta del agente de autenticación.
 - b. En el campo **Confirmar contraseña**, confirme la contraseña introducida en el paso anterior.
8. Seleccione la casilla de verificación **Editar la regla de cambio de contraseña en la autenticación en el Agente de autenticación** si desea que Kaspersky Endpoint Security sustituya por el siguiente valor el valor del parámetro de cambio de contraseña de todas las cuentas del Agente de autenticación creadas a partir de la cuenta de Microsoft Windows que lleva el nombre indicado en el campo **Cuenta de Windows**.
9. Especifique el valor del parámetro de cambio de contraseña al autenticarse en el Agente de autenticación.
10. Seleccione la casilla de verificación **Modificar la configuración de la autenticación basada en certificado** para hacer editable la configuración de la autenticación en función del certificado electrónico de un token o una tarjeta inteligente.
11. Seleccione la casilla de verificación **Autorizar la autenticación basada en certificado** si desea que la aplicación solicite al usuario la introducción de la contraseña al token o a la tarjeta inteligente conectada al equipo durante el proceso de autenticación para acceder a los discos duros cifrados.
12. Si seleccionó la casilla de verificación **Autorizar la autenticación basada en contraseña** durante el paso anterior, haga clic en el botón **Examinar** y seleccione el archivo del certificado electrónico de la tarjeta inteligente o el token en la ventana **Seleccionar el archivo de certificado**.
13. Seleccione la casilla de verificación **Modificar la descripción de comandos** y modifique la descripción de los comandos si desea que Kaspersky Endpoint Security cambie la descripción de los comandos de todas las cuentas del Agente de autenticación que se hayan creado con la cuenta de Microsoft Windows que lleva el nombre que se indica en el campo **Cuenta de Windows**.
14. Seleccione la casilla de verificación **Editar la regla de acceso a la autenticación en el Agente de autenticación** si desea que Kaspersky Endpoint Security cambie la regla de acceso del usuario a la autenticación en el Agente de autenticación por el valor especificado más abajo para todas las cuentas del Agente de autenticación creadas con la cuenta de Microsoft Windows que lleva el nombre indicado en el campo **Cuenta de Windows**.
15. Especifique la regla para acceder al diálogo de autenticación en el Agente de autenticación.
16. En la ventana **Modificar cuenta de usuario**, haga clic en **Aceptar**.

Agregar un comando para eliminar una cuenta del Agente de autenticación

Para agregar un comando a fin de eliminar una cuenta del Agente de autenticación:

1. En la sección **Configuración** de la ventana **Propiedades: <nombre de la tarea de administración de la cuenta del Agente de autenticación>**, abra el menú contextual del botón **Agregar** y seleccione **Comando de modificación de cuentas**.
Se abre la ventana **Eliminar cuenta de usuario**.
2. En el campo **Cuenta de Windows** de la ventana **Eliminar cuenta de usuario**, especifique el nombre de la cuenta de usuario de Microsoft Windows que se utilizó para crear la cuenta del Agente de autenticación que desea eliminar. Para ello, introduzca el nombre de la cuenta manualmente o haga clic en el botón **Seleccionar**.

3. Si ha introducido el nombre de una cuenta de usuario de Microsoft Windows manualmente, haga clic en el botón **Autorizar** para establecer el identificador de seguridad (SID) de la cuenta de usuario.

Si prefiere no establecer el identificador de seguridad (SID) por medio del botón **Autorizar**, se establecerá el SID en el momento en el que se realice la tarea en el equipo.

Establecer el SID de la cuenta de usuario de Microsoft Windows en el momento en el que se agrega un comando de eliminación de cuentas del Agente de autenticación resulta muy práctico para asegurarse de que el nombre de la cuenta de usuario de Microsoft Windows que se ha introducido manualmente es correcto. La tarea de grupo de administración de la cuenta del Agente de autenticación no finaliza de forma correcta si la cuenta de usuario de Microsoft Windows que se ha introducido no existe o pertenece a un dominio no confiable.

4. En la ventana **Eliminar cuenta de usuario**, haga clic en **Aceptar**.

Restaurar las credenciales de la cuenta del Agente de autenticación

Estas instrucciones están destinadas a los usuarios de equipos cliente donde se haya instalado Kaspersky Endpoint Security.

Para restaurar el nombre de usuario y la contraseña de una cuenta del Agente de autenticación:

1. El Agente de autenticación se carga en un equipo que dispone de discos duros cifrados antes de que se cargue el sistema operativo. En la interfaz del Agente de autenticación, pulse **¿Ha olvidado su contraseña?** para iniciar el proceso de restauración del nombre de usuario y la contraseña de una cuenta del Agente de autenticación.
2. Siga las instrucciones del Agente de autenticación con el fin de obtener unidades de solicitud para restaurar el nombre de usuario y la contraseña de la cuenta del Agente de autenticación.
3. Proporcione al administrador de la LAN de su empresa el contenido de los bloques de solicitud y el nombre del equipo.
4. Introduzca las secciones de respuesta a la solicitud de restauración del nombre de usuario y de la contraseña de la cuenta del Agente de autenticación, las cuales le [ha generado y proporcionado](#) el administrador de su red de área local.
5. Introduzca la nueva contraseña de la cuenta del Agente de autenticación y confírmela.

El nombre de usuario de la cuenta del Agente de autenticación se define por medio de la respuesta a las solicitudes de restauración del nombre de usuario y de la contraseña de la cuenta del Agente de autenticación.

Una vez que haya introducido y confirmado la nueva contraseña de la cuenta del Agente de autenticación, esta se guardará y se le concederá acceso a discos duros cifrados.

Responder a un usuario que solicita restaurar las credenciales de la cuenta del Agente de autenticación

Para crear y enviar al usuario las secciones de la respuesta a la solicitud de la restauración del nombre de usuario y de la contraseña de una cuenta del Agente de autenticación:

1. Abra la consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración que incluye el equipo del usuario que ha solicitado la restauración del nombre de usuario y la contraseña de la cuenta del Agente de autenticación.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En la pestaña **Dispositivos**, seleccione el equipo del usuario que ha solicitado la restauración del nombre de usuario y la contraseña de una cuenta del Agente de autenticación, y haga clic con el botón derecho del ratón para abrir el menú contextual.
5. En el menú contextual, seleccione la opción **Conceder acceso a dispositivos y datos en modo sin conexión**. Se abre la ventana **Conceder acceso a dispositivos y datos en modo offline**.
6. En la ventana **Conceder acceso a dispositivos y datos en modo sin conexión**, seleccione la pestaña **Agente de autenticación**.
7. En la sección **Algoritmo de cifrado en uso**, seleccione el tipo de algoritmo de cifrado.
8. En la lista desplegable **Cuenta**, seleccione el nombre de la cuenta del Agente de autenticación creada para el usuario que está solicitando la recuperación del nombre y la contraseña de la cuenta del Agente de autenticación.
9. En la lista desplegable **Disco duro**, seleccione el disco duro cifrado para el cual debe recuperar el acceso.
10. En la sección **Solicitud del usuario**, introduzca los bloques de solicitud que ha establecido el usuario.
El contenido de las secciones de la respuesta a la solicitud del usuario para recuperar el nombre de usuario y la contraseña de la cuenta del Agente de autenticación se mostrará en el campo **Clave de acceso**.
11. Establezca el contenido de los bloques de respuesta al usuario.

Visualización de los detalles del cifrado de datos

Esta sección describe la visualización de los detalles del cifrado de datos.

Acerca del estado del cifrado

Mientras que las tareas de cifrado y descifrado están en curso, Kaspersky Endpoint Security envía a Kaspersky Security Center información sobre el estado de los parámetros del cifrado aplicados a los equipos cliente.

Se pueden dar los siguientes valores del estado del cifrado:

- *Directiva no definida*. Una directiva de Kaspersky Security Center no se ha definido para el equipo.
- *Cifrado/descifrado en curso*. El cifrado y el descifrado de datos está en curso en el equipo.
- *Error*. Se ha producido un error durante el cifrado o descifrado de datos del equipo.
- *Reinicio necesario*. El sistema operativo tiene que ser reanudado para iniciar o acabar el cifrado o el descifrado de los datos en el equipo.

- *De conformidad con la directiva.* El cifrado y/o el descifrado de los datos en el equipo se ha terminado usando la configuración del cifrado especificada en la directiva de Kaspersky Security Center aplicada al equipo.
- *Cancelada por el usuario.* El usuario ha rechazado confirmar la operación de cifrado del archivo en la unidad extraíble.
- *No compatible.* La funcionalidad de cifrado de datos no está disponible en el equipo.

Ver el estado de cifrado

Para ver el estado del cifrado de los datos del equipo:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración al que pertenece el equipo pertinente.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
La pestaña **Dispositivos** del espacio de trabajo muestra las propiedades de los equipos del grupo de administración seleccionado.
4. En la pestaña **Dispositivos** del espacio de trabajo, mueva la barra de desplazamiento hacia la derecha.
La columna **Estado de cifrado** muestra el estado del cifrado de los datos de los equipos que pertenecen al grupo de administración seleccionado. Este estado se constituye en función en la información sobre el cifrado de archivos de las unidades de disco locales del equipo, el cifrado de los discos duros del equipo y el cifrado de las unidades extraíbles conectadas al equipo.

Ver el estado de cifrado en los paneles de información de Kaspersky Security Center

Para ver el estado del cifrado en los paneles de información de Kaspersky Security Center:

1. Abra la consola de administración de Kaspersky Security Center.
2. En el árbol de la consola, seleccione el nodo **Servidor de Administración – <Nombre del equipo>**.
3. En el espacio de trabajo situado a la derecha del árbol de la consola de administración, seleccione la pestaña **Estadísticas**.
4. Cree una nueva página con paneles de información que contengan estadísticas de cifrado de datos. Para ello:
 - a. En la pestaña **Estadísticas**, haga clic en el botón **Personalizar vista**.
Se abre la ventana **Propiedades: Estadísticas**.
 - b. En la ventana **Propiedades: Estadísticas**, haga clic en **Agregar**.
Se abre la ventana **Propiedades: Página nueva**.
 - c. En la sección **General** de la página **Propiedades: Página nueva**, introduzca el nombre de la página.

- d. En la sección **Paneles de información**, haga clic en el botón **Agregar**.
Se abre la ventana **Panel de información nuevo**.
- e. En la ventana **Panel de información nuevo** del grupo **Estado de protección**, seleccione el elemento **Cifrado del dispositivo**.
- f. Haga clic en **Aceptar**.
Se abre la ventana **Propiedades: Control de cifrado**.
- g. En caso de ser necesario, modifique la configuración del panel de información. Para ello, utilice las secciones **Ver y Dispositivos** de la ventana **Propiedades: Cifrado del dispositivo**.
- h. Haga clic en **Aceptar**.
- i. Repita los pasos d-h del proceso, seleccionando el elemento **Cifrado de unidades extraíbles** en la sección **Estado de protección** de la ventana **Panel de información nuevo**.
Los paneles de información que se agregan aparecen en la lista **Paneles de información** de la ventana **Propiedades: Página nueva**.
- j. En la ventana **Propiedades: Página nueva**, haga clic en **Aceptar**.
El nombre de la página que incluye los paneles de información creados en el paso anterior aparece en la lista **Páginas** de la ventana **Propiedades: Estadísticas**.
- k. En la ventana **Propiedades: Estadísticas**, haga clic en **Cerrar**.

5. En la pestaña **Estadísticas**, abra la página creada en los pasos anteriores del proceso.

Aparecen los paneles de información que muestran el estado del cifrado de los equipos y de las unidades extraíbles.

Ver errores de cifrado de archivos en unidades del equipo local

Para ver los errores del cifrado del archivo en unidades del equipo local:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración que incluye el equipo cliente cuya lista de errores de cifrado de archivos desea ver.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En la pestaña **Dispositivos**, seleccione el nombre del equipo en la lista y haga clic con el botón derecho del ratón para abrir el menú contextual.
5. Realice una de las siguientes acciones:
 - En el menú contextual del equipo, seleccione **Protección**.
 - En el menú contextual del equipo, seleccione el elemento **Propiedades**. En la ventana **Propiedades: <nombre del equipo>**, seleccione la sección **Protección**.
6. En la sección **Protección** de la ventana **Propiedades: <nombre del equipo>**, haga clic en el enlace **Ver la lista de errores de cifrado de datos** para abrir la ventana **Errores de cifrado de datos**.

Esta ventana muestra la información de los errores de cifrado de archivos de las unidades del equipo local. Cuando se corrige un error, Kaspersky Security Center elimina la información del error de la ventana **Errores de cifrado de datos**.

Visualización del informe del cifrado de datos

Para ver el informe del cifrado de datos:

1. Abra la consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Informes**.
3. Haga clic en el botón **Crear plantilla de informe**.
Se inicia el Asistente de plantillas de informe.
4. Siga los pasos del Asistente de plantillas de informe. En la ventana **Seleccione el tipo de plantilla de informe** de la sección **Otro**, seleccione uno de los siguientes elementos:
 - **Informe de estado de cifrado de dispositivo administrado.**
 - **Informe de cifrado de datos de dispositivo almacenado.**
 - **Informe de los errores de cifrado.**
 - **Informe de acceso bloqueado a archivos cifrados.**

Una vez ha ya terminado con el Asistente de nueva plantilla de informe, la nueva plantilla de informe aparecerá en la tabla, en la pestaña **Informes**.

5. Seleccione la plantilla del informe que se creó en los pasos anteriores de las instrucciones.

Se inicia el proceso de generación de informes. El informe se muestra en una nueva ventana.

Administración de archivos con una funcionalidad de cifrado de archivos limitada

Cuando se aplica la directiva de Kaspersky Security Center y los archivos se cifran, Kaspersky Endpoint Security recibe una clave de cifrado para acceder directamente a los archivos cifrados. Al utilizar esta clave de cifrado, un usuario que trabaje con una cuenta de Windows que se encontrara activa durante el cifrado de archivos podrá acceder a dichos archivos directamente. Los usuarios que trabajen con cuentas de Windows que no se encontraran activas durante el cifrado de archivos deberán conectarse a Kaspersky Security Center para acceder a los archivos cifrados.

Es posible que los archivos cifrados no sean accesibles en las siguientes circunstancias:

- El equipo del usuario almacena las claves de cifrado, pero no existe conexión con Kaspersky Security Center para administrar las claves. En este caso, el usuario debe solicitar acceso a los archivos cifrados al administrador de la red de área local.

Si no existe acceso a Kaspersky Security Center, debe hacer lo siguiente:

- solicitar una clave de acceso para acceder a archivos cifrados en discos duros del equipo;
- para acceder a archivos cifrados almacenados en unidades extraíbles, deberá solicitar claves de acceso separadas para los archivos cifrados en cada unidad extraíble.
- Los componentes de cifrado se eliminan desde el equipo del usuario. En este evento, el usuario puede abrir archivos cifrados en unidades locales y extraíbles, pero el contenido de esos archivos aparecerá cifrado.

El usuario puede trabajar con archivos cifrados en las siguientes circunstancias:

- Los archivos se encuentran dentro de [paquetes cifrados](#) creados en un equipo con Kaspersky Endpoint Security.
- Los archivos se almacenan en unidades extraíbles en las cuales se permitió el [modo portátil](#).

Acceso a archivos cifrados sin conexión a Kaspersky Security Center

Estas instrucciones están destinadas a los usuarios de equipos cliente donde se haya instalado Kaspersky Endpoint Security.

Para acceder a archivos cifrados sin conexión a Kaspersky Security Center:

1. Intente acceder al archivo cifrado pertinente.


Si no hay conexión a Kaspersky Security Center cuando intenta acceder un archivo que se almacene en una unidad local del equipo, Kaspersky Endpoint Security genera un archivo con una solicitud del acceso a todos los archivos cifrados que se almacenen en las unidades del equipo local. Si intenta acceder a un archivo almacenado en una unidad extraíble, Kaspersky Endpoint Security genera un archivo que solicita el acceso a todos los archivos cifrados almacenados en la unidad extraíble. Se abre la ventana **Acceso a los archivos bloqueado**.

2. Envíe el archivo que contiene la solicitud de acceso a archivos cifrados al administrador de la red de área local. Para ello, siga uno de estos pasos:

- Para enviar al administrador de la red de área local el archivo por el cual se solicita el acceso a los archivos cifrados por medio de correo electrónico, haga clic en el botón **Enviar por correo electrónico**.
- Para guardar el archivo de solicitud de acceso a los archivos cifrados y entregarlo al administrador de la red de área local mediante otro método, haga clic en el botón **Guardar**.

3. Obtenga el archivo de claves para acceder a archivos cifrados que su administrador de red de área local le haya [creado y proporcionado](#).

4. Active la clave para acceder a los archivos cifrados de una de las siguientes maneras:

- En cualquier administrador de archivos, seleccione el archivo de la clave para acceder a archivos cifrados. Haga doble clic para abrirlo.
- Haga lo siguiente:
 - a. Abra la ventana principal de Kaspersky Endpoint Security.
 - b. Haz clic en el botón . Esto abre la ventana **Eventos**.

c. Seleccione la pestaña **Estado de acceso a archivos y dispositivos**.

La pestaña contiene una lista de todas las solicitudes de acceso a archivos cifrados.

d. Seleccione la solicitud para la cual ha recibido el fichero llave para acceder a archivos cifrados.

e. Para cargar el archivo de claves proporcionado para acceder a los archivos cifrados, haga clic en **Examinar**.

Se abre el cuadro de diálogo estándar **Seleccionar archivo de claves de acceso** de Microsoft Windows.

f. En la ventana **Seleccionar archivo de claves de acceso** estándar de Microsoft Windows, seleccione el archivo proporcionado por los administradores con la extensión .kesdr y cuyo nombre coincida con el nombre del archivo de solicitud del acceso.

g. Haga clic en el botón **Abrir**.

h. En la ventana **Eventos**, haga clic en **Aceptar**.

Si un archivo con una solicitud del acceso a los archivos cifrados se genera durante un intento de acceder un archivo que se almacene en una unidad local del equipo, Kaspersky Endpoint Security concede el acceso a todos los archivos cifrados que se almacenen en las unidades del equipo local. Si se genera un archivo de solicitud de acceso a archivos cifrados durante un intento de acceso a un archivo almacenado en una unidad extraíble, Kaspersky Endpoint Security proporciona acceso a todos los archivos cifrados almacenados en la unidad extraíble. Para acceder a archivos cifrados almacenados en otras unidades extraíbles, obtenga un archivo de claves de acceso independiente para cada unidad extraíble.

Conceder acceso a archivos cifrados sin conexión a Kaspersky Security Center

Para conceder al usuario acceso a archivos cifrados sin conexión a Kaspersky Security Center:

1. Abra la consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración que incluye el equipo del usuario que solicita acceso a archivos cifrados.

3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.

4. En la pestaña **Dispositivos**, seleccione el equipo que pertenece al usuario que solicita acceso a archivos cifrados y haga clic con el botón derecho del ratón para abrir el menú contextual.

5. En el menú contextual, seleccione la opción **Conceder acceso a dispositivos y datos en modo sin conexión**.

Se abre la ventana **Conceder acceso a dispositivos y datos en modo offline**.

6. En la ventana **Conceder acceso a dispositivos y datos en modo offline**, seleccione la pestaña **Cifrado**.

7. En la pestaña **Cifrado**, haga clic en el botón **Examinar**.

Se abre el cuadro de diálogo estándar **Seleccionar archivo de solicitud de acceso** de Microsoft Windows.

8. En la ventana **Seleccionar archivo de solicitud de acceso**, especifique la ruta al archivo de solicitud recibido del usuario y haga clic en **Abrir**.

Kaspersky Security Center genera un archivo de claves para acceder a los archivos cifrados. La pestaña **Cifrado** muestra la información detallada de la solicitud del usuario.

9. Realice una de las siguientes acciones:

- Para enviar el archivo de claves de acceso generado al usuario por medio de correo electrónico, haga clic en el botón **Enviar por correo electrónico**.
- Para guardar el archivo de claves de acceso de los archivos cifrados y entregárselo al usuario por medio de otro método, haga clic en el botón **Guardar**.

Modificación de plantillas de mensajes de acceso a archivos cifrados

Para modificar las plantillas de los mensajes de acceso a archivos cifrados:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta con el nombre del grupo de administración para el que desea editar las plantillas de los mensajes de solicitud del acceso a archivos cifrados.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Cifrado de datos**, seleccione el apartado **Configuración común de cifrado**.
7. En la sección **Plantillas**, haga clic en el botón **Plantillas**.
Se abre la ventana **Plantillas**.
8. Haga lo siguiente:
 - Si desea editar la plantilla del mensaje del usuario, seleccione la pestaña **Mensaje del usuario**. Se abre la ventana **Acceso a archivo denegado** cuando el usuario intenta acceder a un archivo cifrado y no existe ninguna clave para acceder a archivos cifrados disponible en el equipo. Al hacer clic en el botón **Enviar por correo electrónico** de la ventana **Acceso a archivo denegado**, se crea un mensaje de usuario de forma automática. Este mensaje se envía al administrador de la red de área local corporativa junto con el archivo de solicitud de acceso a archivos cifrados.
 - Si desea editar la plantilla del mensaje del administrador, seleccione la pestaña **Mensaje del administrador**. Este mensaje de correo electrónico se crea automáticamente al hacer clic en el botón **Enviar por correo electrónico** de la ventana **Conceder acceso a los archivos cifrados** y se envía al usuario una vez que se le concede acceso a los archivos cifrados.
9. Modifique las plantillas de mensajes.
Puede usar el botón **Predeterminado** y la lista desplegable **Variable**.
10. Haga clic en **Aceptar**.

11. Para guardar los cambios, en la ventana **Propiedades: <Nombre de directiva>**, haga clic en **Aceptar**.

Trabajar con dispositivos cifrados cuando no hay acceso a estos

Obtener acceso a los dispositivos cifrados

Es posible que se requiera a un usuario solicitar acceso a dispositivos cifrados en los siguientes casos:

- El disco duro se cifró en un equipo diferente.
- La clave de cifrado para un dispositivo no está en el equipo (por ejemplo, después del primer intento de acceder a la unidad extraíble cifrada en el equipo), y el equipo no está conectado a Kaspersky Security Center. Después de que el usuario ha aplicado la clave de acceso al dispositivo cifrado, Kaspersky Endpoint Security guarda la clave de cifrado en el equipo del usuario y permite el acceso a este dispositivo después de sucesivos intentos de acceso, incluso si no hay conexión con Kaspersky Security Center.

El acceso a dispositivos cifrados se puede obtener de la siguiente manera:

1. El usuario [usa la interfaz de aplicación Kaspersky Endpoint Security para crear un archivo de solicitud de acceso](#) con la extensión kesdc y lo envía al administrador de la red de área local corporativa.
2. El administrador [usa la Consola de administración de Kaspersky Security Center para crear un archivo de clave de acceso](#) con la extensión kesdr y lo envía al usuario.
3. El usuario [aplica la clave de acceso](#).

Restauración de datos de dispositivos cifrados

Un usuario puede usar la [Utilidad de restauración de dispositivos cifrados](#) (denominada en lo sucesivo la Utilidad de restauración) para trabajar con dispositivos cifrados. Esto se puede requerir en los siguientes casos:

- Falló el procedimiento para usar una clave de acceso para obtener acceso.
- Los componentes de cifrado no se han instalado en el equipo con el dispositivo cifrado.

Los datos necesarios para restaurar el acceso a dispositivos cifrados usando la Utilidad de restauración permanecen durante un tiempo sin cifrar en la memoria del equipo del usuario. Para reducir el riesgo de acceso no autorizado a estos datos, se aconseja restaurar el acceso a dispositivos cifrados en equipos de confianza.

Los datos en dispositivos cifrados se pueden restaurar de la siguiente manera:

1. El usuario [usa la Utilidad de restauración para crear un archivo de solicitud de acceso](#) con la extensión fdertc y lo envía al administrador de la red de área local corporativa.
2. El administrador [usa la Consola de administración de Kaspersky Security Center para crear un archivo de clave de acceso](#) con la extensión fdertr y lo envía al usuario.
3. El usuario [aplica la clave de acceso](#).

Para restaurar datos de discos duros de sistemas cifrados, el usuario también puede especificar las credenciales de la cuenta del Agente de autenticación en la Utilidad de restauración. Si los metadatos de la cuenta del Agente de autenticación están dañados, el usuario debe completar el procedimiento de restauración con un archivo de solicitud de acceso.

Antes de restaurar el acceso a dispositivos cifrados, se recomienda cancelar la directiva de cifrado de Kaspersky Security Center en el equipo donde esta operación deba llevarse a cabo. Esto evita que la unidad vuelva a cifrarse.

Obtención de acceso a dispositivos cifrados a través de la interfaz de aplicación

Estas instrucciones están destinadas a los usuarios de equipos cliente donde se haya instalado Kaspersky Endpoint Security.


Para obtener acceso a dispositivos cifrados a través de la interfaz de la aplicación:

1. Intente acceder al archivo cifrado que necesita.

Se abre la ventana **El acceso a los datos está bloqueado**.


2. Envíe al administrador de la red de área local corporativa el archivo de solicitud de acceso con la extensión kesdc para el dispositivo cifrado. Para ello, siga uno de estos pasos:

- Para enviar por correo electrónico al administrador de la red de área local corporativa el archivo de solicitud de acceso generado para el dispositivo cifrado, haga clic en el botón **Enviar por correo electrónico**.
- Para guardar el archivo de solicitud de acceso para el dispositivo cifrado y entregarlo al administrador de la red de área local corporativa usando otro método, haga clic en el botón **Guardar**.

Si ha cerrado la ventana **El acceso a los datos está bloqueado** sin guardar el archivo de solicitud de acceso o sin enviarlo al administrador de la red de área local corporativa, puede hacerlo en cualquier momento en la ventana **Eventos**, en la pestaña **Estado de acceso a archivos y dispositivos**. Para abrir esta ventana, haga clic en el botón  en la ventana principal de la aplicación.

3. Obtenga y guarde el archivo de clave de acceso del dispositivo cifrado que se ha [creado y que le ha proporcionado](#) el administrador de la red de área local corporativa.

4. Use uno de los siguientes métodos para aplicar la clave de acceso para acceder al dispositivo cifrado:

- En cualquier gestor de archivos, busque el archivo de clave de acceso del dispositivo cifrado y haga doble clic en él para abrirlo.
- Haga lo siguiente:
 - a. Abra la ventana principal de Kaspersky Endpoint Security.
 - b. Al hacer clic en el botón , se abre la ventana **Exclusiones**.
 - c. Seleccione la pestaña **Estado de acceso a archivos y dispositivos**.

La pestaña contiene una lista de todas las solicitudes de acceso a archivos y dispositivos cifrados.

- d. Seleccione la solicitud para la cual ha recibido el archivo de clave de acceso para acceder al dispositivo cifrado.
- e. Para cargar el archivo de clave de acceso recibido para acceder a los archivos cifrados, haga clic en **Examinar**.
Se abre el cuadro de diálogo estándar **Seleccionar archivo de claves de acceso** de Microsoft Windows.
- f. En la ventana **Seleccionar archivo de claves de acceso** estándar de Microsoft Windows, seleccione el archivo proporcionado por el administrador con la extensión .kesdr y nombre que coincida con el del archivo de solicitud de acceso correspondiente al dispositivo cifrado.
- g. Haga clic en el botón **Abrir**.
- h. En la ventana **Estado de acceso a archivos y dispositivos**, haga clic en **Aceptar**.

Como resultado, Kaspersky Endpoint Security concede acceso al dispositivo cifrado.

Conceder al usuario acceso a dispositivos cifrados

Conceder al usuario acceso a un dispositivo cifrado:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración que incluye el equipo del usuario que solicita acceso al dispositivo cifrado.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En la pestaña **Dispositivos**, seleccione el equipo que pertenece al usuario que solicita acceso al dispositivo cifrado y haga clic con el botón derecho del ratón para abrir el menú contextual.
5. En el menú contextual, seleccione la opción **Conceder acceso a dispositivos y datos en modo sin conexión**.
Se abre la ventana **Conceder acceso a dispositivos y datos en modo offline**.
6. En la ventana **Conceder acceso a dispositivos y datos en modo offline**, seleccione la pestaña **Cifrado**.
7. En la pestaña **Cifrado**, haga clic en el botón **Examinar**.
Se abre el cuadro de diálogo estándar **Seleccionar archivo de solicitud de acceso** de Microsoft Windows.
8. En la ventana **Seleccionar archivo de solicitud de acceso**, especifique la ruta al archivo de solicitud con la extensión kesdc, que recibió del usuario.
9. Haga clic en el botón **Abrir**.
Kaspersky Security Center genera un archivo de clave de acceso al dispositivo cifrado con la extensión kesdr. La pestaña **Cifrado** muestra la información detallada de la solicitud del usuario.
10. Realice una de las siguientes acciones:
 - Para enviar el archivo de claves de acceso generado al usuario por medio de correo electrónico, haga clic en el botón **Enviar por correo electrónico**.

- Para guardar el archivo de claves de acceso del dispositivo cifrado y entregárselo al usuario por medio de otro método, haga clic en el botón **Guardar**.

Proporcionar a un usuario una clave de recuperación para discos duros cifrados con BitLocker

Para enviar a un usuario una clave de recuperación para un disco duro del sistema que se cifró con BitLocker:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración que incluye el equipo del usuario que solicita acceso a la unidad cifrada.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En la pestaña **Dispositivos**, seleccione el nombre del equipo que pertenece al usuario que solicita acceso a la unidad cifrada.
5. Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Conceder acceso a dispositivos y datos en modo sin conexión**.
Se abre la ventana **Conceder acceso a dispositivos y datos en modo offline**.
6. En la ventana **Conceder acceso a dispositivos y datos en modo sin conexión**, seleccione la pestaña **Acceso a una unidad de sistema protegida por BitLocker**.
7. Solicite al usuario el ID de la clave de recuperación indicado en la ventana de introducción de la contraseña de BitLocker y compárelo con el ID del campo **ID de clave de recuperación**.

Si los ID no coinciden, esta clave no es válida para restaurar el acceso a la unidad del sistema especificada. Asegúrese de que el nombre del equipo seleccionado coincide con el nombre del equipo del usuario.

8. Envíe al usuario la clave que se indica en el campo **Clave de recuperación**.

Para enviar a un usuario una clave de recuperación para un disco duro que no pertenece al sistema y se cifró con BitLocker:

1. Abra la consola de administración de Kaspersky Security Center.
2. En el árbol de la consola de administración, seleccione la carpeta **Avanzado** → **Cifrado y protección de datos** → **Dispositivos cifrados**.
El espacio de trabajo muestra una lista de dispositivos cifrados.
3. En el espacio de trabajo, seleccione el dispositivo cifrado al cual debe restaurar el acceso.
4. Haga clic con el botón derecho del ratón para mostrar el menú contextual y seleccione **Obtener clave de acceso para el dispositivo cifrado específico**.
Esto abre la ventana **Restaurar acceso al disco cifrado con BitLocker**.
5. Solicite al usuario el ID de la clave de recuperación indicado en la ventana de introducción de la contraseña de BitLocker y compárelo con el ID del campo **ID de clave de recuperación**.


Si los ID no coinciden, esta clave no es válida para restaurar el acceso a la unidad especificada. Asegúrese de que el nombre del equipo seleccionado coincide con el nombre del equipo del usuario.

6. Envíe al usuario la clave que se indica en el campo **Clave de recuperación**.

Creación del archivo ejecutable de la Utilidad de restauración

Estas instrucciones están destinadas a los usuarios de equipos cliente donde se haya instalado Kaspersky Endpoint Security.

Para crear el archivo ejecutable de la Utilidad de restauración:

1. Abra la [ventana principal de la aplicación](#).
2. Haga clic en el botón  situado en la esquina inferior izquierda de la ventana principal de la aplicación para abrir la ventana **Soporte**.
3. En la ventana **Soporte**, haga clic en el botón **Restaurar dispositivo cifrado**.
Se ejecuta la Utilidad de restauración de dispositivos cifrados.
4. Haga clic en el botón **Crear Utilidad de restauración independiente** de la ventana de la Utilidad de restauración.
Se abre la ventana **Creación de una Utilidad de restauración independiente**.
5. En la ventana **Guardar en**, escriba de forma manual la ruta a la carpeta en la que desea guardar el archivo ejecutable de la Utilidad de restauración o haga clic en el botón **Examinar**.
6. Haga clic en **Aceptar** en la ventana **Creación de una Utilidad de restauración independiente**.
El archivo ejecutable de la Utilidad de restauración (fdert.exe) se guarda en la carpeta seleccionada.

Restaurar datos en dispositivos cifrados por medio de la Utilidad de restauración

Estas instrucciones están destinadas a los usuarios de equipos cliente donde se haya instalado Kaspersky Endpoint Security.

Para restaurar el acceso a un dispositivo cifrado por medio de la Utilidad de restauración:

1. Ejecute la Utilidad de restauración de una de las siguientes formas:
 - Haga clic en el botón  de la ventana principal de Kaspersky Endpoint Security para abrir la ventana **Soporte** y, a continuación, haga clic en el botón **Restaurar dispositivo cifrado**.
 - Ejecute el archivo fdert.exe de la Utilidad de restauración. [Kaspersky Endpoint Security crea este archivo](#).

2. En la ventana de la Utilidad de restauración, en la lista desplegable **Seleccionar dispositivo**, seleccione el dispositivo cifrado cuyo acceso desea restaurar.

3. Haga clic en el botón **Analizar** para permitir a la utilidad definir qué acciones se deben llevar a cabo en el dispositivo: si se debe desbloquear o descifrar.

Si el equipo tiene acceso a la funcionalidad de cifrado de Kaspersky Endpoint Security, la Utilidad de restauración le pedirá a usted que desbloquee el dispositivo. Aunque el desbloqueo de un dispositivo no lo descifra, puede accederse a este directamente como consecuencia de estar desbloqueado. Si el equipo no tiene acceso a la funcionalidad de cifrado de Kaspersky Endpoint Security, la Utilidad de restauración le pedirá a usted que descifre el dispositivo.

4. Haga clic en el botón **Corregir MBR** si el diagnóstico del disco duro del sistema cifrado ha devuelto un mensaje acerca de que hay problemas relacionados con el registro de arranque principal (MBR) del dispositivo.

El arreglo del registro de arranque principal del dispositivo puede acelerar el proceso de recopilación de información necesario para desbloquear o descifrar el dispositivo.

5. Haga clic en el botón **Desbloquear** o **Descifrar**, según los resultados del diagnóstico.

Se abre la ventana **Configuración de desbloqueo del dispositivo** o **Configuración del descifrado de dispositivos**.

6. Si desea restaurar datos usando una cuenta del Agente de autenticación:

a. Seleccione la opción **Usar configuración de la cuenta del Agente autenticación**.

b. En los campos **Nombre** y **Contraseña**, especifique las credenciales de la cuenta del Agente de autenticación.

Este método solo es posible al restaurar datos en un disco duro del sistema. Si el disco duro del sistema está dañado y los datos de la cuenta del Agente de autenticación se han perdido, debe obtener una clave de acceso del administrador de la red de área local corporativa para restaurar datos en un dispositivo cifrado.

7. Si desea usar una clave de acceso para restaurar datos:

a. Seleccione la opción **Especificar manualmente la clave de acceso al dispositivo**.

b. Haga clic en el botón **Recibir clave de acceso**.

c. Se abre la ventana **Recibir clave de acceso al dispositivo**.

d. Haga clic en el botón **Guardar** y seleccione la carpeta en la cual va a guardar el archivo de solicitud de acceso con la extensión fdertc.

e. Envíe el archivo de solicitud de acceso al administrador de la red de área local corporativa.

No cierre la ventana **Recibir la clave de acceso al dispositivo** hasta que haya recibido la clave de acceso. Si esta ventana se abre de nuevo, no podrá aplicar la clave de acceso que el administrador había creado anteriormente.

f. Obtenga y guarde el archivo de clave de acceso que [creó y le proporcionó](#) el administrador de la red de área local corporativa.

g. Haga clic en el botón **Cargar** y seleccione el archivo de clave de acceso con la extensión fdetr en la ventana que se abre.

8. Si está descifrando un dispositivo, también debe especificar la otra configuración de descifrado en la ventana **Configuración del descifrado de dispositivos**. Para ello:

- Especifique la parte que va a descifrar:
 - Si desea descifrar el dispositivo completo, seleccione la opción **Descifrar todo el dispositivo**.
 - Si desea descifrar una parte de los datos de un dispositivo, seleccione la opción **Descifrar áreas particulares del dispositivo** y use los campos **Iniciar** y **Finalizar** para especificar los límites de la parte que se va a descifrar.
- Seleccione la ubicación para escribir los datos descifrados:
 - Si desea que los datos del dispositivo original se vuelvan a escribir con los datos descifrados, borre la casilla de verificación **Guardar datos en el archivo después del descifrado**.
 - Si desea guardar datos descifrados por separado de los datos cifrados originales, seleccione la casilla de verificación **Guardar datos en el archivo después del descifrado** y use el botón **Examinar** para especificar la ruta en la que desea guardar los datos.

9. Haga clic en **Aceptar**.

Comienza el proceso de descifrado o desbloqueo.

Responder a un usuario que solicita restaurar datos de dispositivos cifrados

Para crear un archivo llave que permita acceder a un dispositivo cifrado y proporcionárselo al usuario:

1. Abra la consola de administración de Kaspersky Security Center.
2. En el árbol de la consola de administración, seleccione la carpeta **Avanzado** → **Cifrado y protección de datos** → **Dispositivos cifrados**.
3. En el espacio de trabajo, seleccione el dispositivo cifrado para el cual desea crear un archivo de clave de acceso y, en el menú contextual del dispositivo, seleccione **Obtener clave de acceso para el dispositivo cifrado específico**.

Si no está seguro para cuál equipo se generó el archivo de solicitud de acceso, en el árbol de la consola de administración, seleccione la carpeta **Avanzado** → **Cifrado y protección de datos** y, en el espacio de trabajo, haga clic en el enlace **Obtener clave de cifrado del dispositivo**.

Se abre la ventana **Permitir el acceso al dispositivo**.

4. Seleccione el algoritmo de cifrado en uso. Para ello, seleccione una de las siguientes opciones:
 - **AES256**, si Kaspersky Endpoint Security se ha instalado desde un paquete de distribución ubicado en la carpeta aes256 del equipo en el que se cifró el dispositivo.
 - **AES56**, si Kaspersky Endpoint Security se ha instalado desde un paquete de distribución ubicado en la carpeta aes56 del equipo en el que se cifró el dispositivo.

5. Haga clic en el botón **Examinar**.

Se abre el cuadro de diálogo estándar **Seleccionar archivo de solicitud de acceso** de Microsoft Windows.

6. En la ventana **Seleccionar archivo de solicitud de acceso**, especifique la ruta al archivo de solicitud con la extensión `fdertc` que recibió del usuario.

7. Haga clic en el botón **Abrir**.

Kaspersky Security Center genera un archivo de clave de acceso con la extensión `fdertr` para acceder al dispositivo cifrado.

8. Realice una de las siguientes acciones:

- Para enviar el archivo de claves de acceso generado al usuario por medio de correo electrónico, haga clic en el botón **Enviar por correo electrónico**.
- Para guardar el archivo de claves de acceso del dispositivo cifrado y entregárselo al usuario por medio de otro método, haga clic en el botón **Guardar**.

Restauración del acceso a los datos cifrados después del error del sistema operativo

Puede restaurar el acceso a los datos después del error del sistema operativo solo con el cifrado de archivos (CA). No puede restaurar el acceso a los datos si se utiliza cifrado de disco completo (CDC).

Para restaurar el acceso a los datos cifrados después del error del sistema operativo:

1. Vuelva a instalar el sistema operativo sin formatear el disco duro.
2. [Instale Kaspersky Endpoint Security](#).
3. Establezca una conexión entre el equipo y el Servidor de administración de Kaspersky Security Center que controló el equipo cuando se cifraron los datos.

Se concederá el acceso a los datos cifrados bajo las mismas condiciones que se aplicaban antes del error del sistema operativo.

Creación de un disco de rescate del sistema operativo

El disco de rescate del sistema operativo puede ser útil cuando no se puede acceder a un disco duro cifrado por alguna razón y el sistema operativo no se puede cargar.

Puede cargar una imagen del sistema operativo Windows por medio del disco de rescate y restaurar el acceso al disco duro cifrado por medio de la Utilidad de restauración incluida en la imagen del sistema operativo.

Para crear un disco de rescate del sistema operativo:

1. [Cree un archivo ejecutable para la Utilidad de restauración de dispositivos cifrados](#).
2. Cree una imagen personalizada del entorno de prearranque de Windows. Mientras tanto, agregue el archivo ejecutable de la Utilidad de restauración a la imagen.
3. Guardar la imagen personalizada del entorno de preinstalación de Windows en medios de arranque como, por ejemplo, un lector de CD o una unidad extraíble.

Consulte los archivos de ayuda de Microsoft para recibir instrucciones sobre la creación de una imagen personalizada del entorno de prearranque de Windows (por ejemplo, en el [recurso Microsoft TechNet](#) ²⁴).

Protección de red

Esta sección contiene información sobre la supervisión del tráfico de red, además de instrucciones sobre cómo configurar los parámetros de los puertos de red supervisados.

Acerca de Protección de red

Durante el funcionamiento de Kaspersky Endpoint Security, componentes como [Antivirus del correo](#), [Antivirus Internet](#) y [Antivirus para chat](#) supervisan los flujos de datos que se transmiten mediante protocolos específicos y que pasan a través de los puertos TCP y UDP que se encuentran abiertos en su equipo. Por ejemplo, Antivirus del correo analiza los datos que se transmiten a través de SMTP, mientras que Antivirus Internet analiza los datos que se transmiten mediante HTTP y FTP.

Kaspersky Endpoint Security divide los puertos TCP y UDP del sistema operativo en varios grupos, según las probabilidades de que se vean en riesgo. Algunos puertos de red se reservan para servicios que puedan ser vulnerables. Se recomienda supervisar estos puertos con más detenimiento, puesto que la probabilidad de que sufran ataques es mayor. Si usa servicios no estándares que dependen de puertos de red no estándares, dichos puertos de red también pueden ser el objetivo de los equipos atacantes. Puede especificar una lista de puertos de red y una lista de aplicaciones que solicitan acceso a la red. De ese modo, estos puertos y aplicaciones reciben una atención especial de los componentes Antivirus del correo, Antivirus Internet y Antivirus para chat mientras supervisan el tráfico de la red.

Configuración de los parámetros de supervisión del tráfico de red

Puede realizar las siguientes acciones para configurar los parámetros de supervisión del tráfico de red:

- Active la vigilancia de todos los puertos de red.
- Cree una lista de puertos de red supervisados.
- Cree una lista de aplicaciones para las que se vigilen todos los puertos de red.

Activación de la vigilancia de todos los puertos de red

Para activar la vigilancia de todos los puertos de red, haga lo siguiente:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, seleccione la sección **Protección antivirus**.
La configuración de la protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Puertos vigilados**, seleccione **Vigilar todos los puertos de red**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Creación de una lista de puertos de red supervisados

Para crear una lista de puertos de red supervisados:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, seleccione la sección **Protección antivirus**.

La configuración de la protección antivirus se muestra en la parte derecha de la ventana.

3. En la sección **Puertos vigilados**, seleccione **Vigilar solo los puertos seleccionados**.

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

Se abre la ventana **Puertos de red**. La ventana **Puertos de red** muestra una lista de puertos que se usan normalmente para la transmisión de correo electrónico y tráfico de red. La lista de puertos de red se incluye en el paquete de Kaspersky Endpoint Security.

5. En la lista de puertos de red, realice la siguiente acción:

- Seleccione las casillas de verificación de los puertos de red que quiera incluir en la lista de puertos de red vigilados.

De forma predeterminada, están seleccionadas las casillas de verificación de todos los puertos de red enumerados en la lista de la ventana **Puertos de red**.

- Desactive las casillas de verificación de los puertos de red que quiera excluir en la lista de puertos de red vigilados.

6. Si no aparece un puerto de red en la lista de puertos de red, agréguelo del siguiente modo:

a. En la lista de puertos de red, haga clic en el enlace **Agregar** para abrir la ventana **Puerto de red**.

b. Introduzca el número de puerto de red en el campo **Puerto**.

c. Introduzca el nombre del puerto de red en el campo **Descripción**.

d. Haga clic en **Aceptar**.

Se cierra la ventana **Puerto de red**. El puerto de red que acaba de crear se muestra al final de la lista de puertos de red.

7. En la ventana **Puertos de red**, haga clic en **Aceptar**.

8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Cuando el protocolo FTP se ejecuta en modo pasivo, la conexión se puede establecer a través de un puerto de red al azar que no se agrega a la lista de puertos de red supervisados. Para proteger estas conexiones, seleccione la casilla de verificación **Vigilar todos los puertos de red** en la sección **Puertos vigilados** o [configure la supervisión de todos los puertos para las aplicaciones](#) que establecen la conexión FTP.

Creación de una lista de aplicaciones para las que se supervisan todos los puertos de red

Puede crear una lista de aplicaciones para las que Kaspersky Endpoint Security supervisa todos los puertos de red.

Recomendamos incluir las aplicaciones que reciben o transmiten datos mediante el protocolo FTP en la lista de aplicaciones para las que Kaspersky Endpoint Security supervisa todos los puertos de red.

Para crear una lista de aplicaciones para las que se supervisan todos los puertos de red:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, seleccione la sección **Protección antivirus**.
La configuración de la protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Puertos vigilados**, seleccione **Vigilar solo los puertos seleccionados**.
4. Haga clic en el botón **Configuración**.
Se abre la ventana **Puertos de red**.
5. Seleccione la casilla de verificación **Supervisar todos los puertos para las aplicaciones especificadas**.
6. En la lista de aplicaciones de la casilla de verificación **Supervisar todos los puertos para las aplicaciones especificadas**, haga lo siguiente:
 - Seleccione las casillas de verificación junto a los nombres de las aplicaciones para las que quiere supervisar todos los puertos de red.
De forma predeterminada, están seleccionadas las casillas de verificación que hay junto a las aplicaciones enumeradas en la lista de la ventana **Puertos de red**.
 - Desactive las casillas de verificación junto a los nombres de las aplicaciones para las que no quiere supervisar todos los puertos de red.
7. Si una aplicación no está incluida en la lista, agréguela del modo siguiente:
 - a. Haga clic en el enlace **Agregar** de la lista de aplicaciones y abra el menú contextual.
 - b. En el menú contextual, seleccione el modo en que se agregará la aplicación a la lista:
 - Para seleccionar la aplicación en la lista de las que están instaladas en el equipo, seleccione el comando **Aplicaciones**. Se abre la ventana **Seleccionar aplicación**, que le permite especificar el nombre de la aplicación.
 - Para especificar la ubicación del archivo ejecutable de la aplicación, seleccione el comando **Examinar**. Se abre la ventana estándar **Abrir** en Microsoft Windows, que le permite especificar el nombre del archivo ejecutable de la aplicación.

La ventana **Aplicación** se abrirá después de que seleccione la aplicación.

- c. En el campo **Nombre**, introduzca el nombre de la aplicación seleccionada.

d. Haga clic en **Aceptar**.

Se cierra la ventana **Aplicación**. La aplicación que ha agregado aparece al final de la lista de aplicaciones.

8. En la ventana **Puertos de red**, haga clic en **Aceptar**.

9. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Actualización de las bases de datos y módulos de la aplicación

Esta sección contiene información sobre las actualizaciones de la base de datos y de los módulos de la aplicación (también llamadas "actualizaciones"), así como instrucciones sobre la configuración de los parámetros de actualización.

Acerca de las actualizaciones de la base de datos y de los módulos de la aplicación

La actualización de las bases de datos y de los módulos de Kaspersky Endpoint Security garantiza una protección actualizada del equipo. Cada día aparecen en todo el mundo nuevos virus y otros tipos de software malicioso (malware). Las bases de datos de Kaspersky Endpoint Security contienen información sobre las amenazas y las maneras de neutralizarlas. Para detectar amenazas rápidamente, es recomendable que actualice regularmente las bases de datos y los módulos de la aplicación.

Las actualizaciones regulares requieren una licencia efectiva. Si no hay ninguna licencia actual, solamente podrá realizar una actualización una vez.

El origen principal de actualizaciones para Kaspersky Endpoint Security son los servidores de actualizaciones de Kaspersky.

Su equipo debe estar conectado a Internet para descargar satisfactoriamente el paquete de actualización de los servidores de actualizaciones de Kaspersky. De forma predeterminada, los parámetros de conexión a Internet se determinan automáticamente. Si utiliza un servidor proxy, puede ser necesario [ajustar los parámetros de conexión](#).

Mientras se lleva a cabo la actualización, se descargan e instalan los siguientes objetos en su equipo:

- Bases de datos de Kaspersky Endpoint Security. La protección del equipo se proporciona por medio de bases de datos que contienen firmas de virus y otras amenazas, así como información sobre la forma de neutralizarlas. Los componentes de protección emplean esta información a la hora de buscar y neutralizar archivos infectados en el equipo. Las bases de datos se actualizan constantemente con registros de nuevas amenazas y métodos para combatirlas. Por tanto, es recomendable que actualice la base de datos con regularidad.
Además de las bases de Kaspersky Endpoint Security, también se actualizan los controladores de red que permiten a los componentes de protección interceptar el tráfico de la red.
- Módulos de la aplicación. Aparte de las bases de datos de Kaspersky Endpoint Security, también puede actualizar los módulos de la aplicación. La actualización de los módulos de la aplicación sirve para solucionar vulnerabilidades en Kaspersky Endpoint Security, agrega nuevas funciones o mejora las existentes.

Durante una actualización, los módulos de la aplicación y las bases de datos del equipo se comparan con los de la versión actualizada en el origen de actualizaciones. Si los módulos de la aplicación y las bases de datos actuales son diferentes de sus respectivas versiones actualizadas, la parte de las actualizaciones que falte se instala en su equipo.

Los archivos de ayuda contextual se pueden actualizar junto con las actualizaciones de los módulos de la aplicación.

Si las bases de datos no están actualizadas, puede que el tamaño del paquete de actualización sea considerable, lo que provocaría un tráfico de Internet adicional (hasta varias docenas de MB).

La información sobre el estado actual de las bases de datos de Kaspersky Endpoint Security se muestra en **Actualización**, en la sección **Tareas** de la pestaña **Protección y control** de la [ventana principal de la aplicación](#).

La información sobre los resultados de la actualización y sobre todos los eventos se producen durante la ejecución de la tarea de actualización se registra en el [informe de Kaspersky Endpoint Security](#).

Acerca de los orígenes de actualizaciones

Un *origen de actualizaciones* es un recurso que contiene actualizaciones de las bases de datos y los módulos de la aplicación de Kaspersky Endpoint Security.

Los orígenes de actualizaciones incluyen el servidor de Kaspersky Security Center y los servidores de actualizaciones de Kaspersky y carpetas locales y en red.

Configuración de los parámetros de actualización

Puede llevar a cabo las siguientes acciones para configurar los parámetros de actualización:

- Agregar nuevos orígenes de actualizaciones.

La lista predeterminada de orígenes de actualizaciones incluye los servidores de actualizaciones de Kaspersky Security Center y Kaspersky. Puede agregar a la lista otros orígenes de actualizaciones. Puede especificar servidores HTTP/FTP o carpetas compartidas como orígenes de actualizaciones.

Si se seleccionan varios recursos como orígenes de actualizaciones, Kaspersky Endpoint Security intenta conectarse a ellos uno después de otro, empieza desde el inicio de la lista y realiza la tarea de actualización al recuperar el paquete de actualización del primer origen disponible.

Si selecciona un recurso ubicado fuera de la LAN como origen de actualizaciones, será necesaria una conexión a Internet para descargar las actualizaciones.

- Seleccione la región del servidor de actualizaciones de Kaspersky.

Si utiliza servidores de actualizaciones de Kaspersky como un origen de actualizaciones, puede elegir la ubicación del servidor de actualizaciones de Kaspersky que se emplee para descargar el paquete de actualización. Kaspersky posee servidores de actualizaciones en varios países. El uso de los servidores de actualizaciones de Kaspersky más cercanos ayuda a reducir el tiempo que se emplea en descargar un paquete de actualización.

De forma predeterminada, la aplicación utiliza información sobre la región actual del registro del sistema operativo.

- Configure la actualización de Kaspersky Endpoint Security desde una carpeta compartida.

Para ahorrar tráfico de Internet, puede configurar las actualizaciones de Kaspersky Endpoint Security para que los equipos de su LAN reciban actualizaciones desde una carpeta compartida. Para ello, uno de los equipos de su LAN recibe un paquete de actualización del servidor de Kaspersky Security Center o de los servidores de actualizaciones de Kaspersky y, a continuación, copia el paquete de actualización descargado en una carpeta compartida. Después, el resto de los equipos de su LAN pueden acceder al paquete de actualización a través de esta carpeta compartida.

- Seleccione el modo de ejecución de la tarea de actualización.

Si no es posible iniciar la tarea de actualización por alguna razón (por ejemplo, el equipo estaba apagado en ese momento), puede configurar la tarea que se ha omitido para que se inicie automáticamente lo antes posible.

Puede retrasar la ejecución de la tarea de actualización después de que se inicie la aplicación si selecciona el modo de ejecución de la tarea de ejecución **Mediante planificación** y si el momento del inicio de Kaspersky Endpoint Security coincide con la planificación del inicio de la tarea de actualización. La tarea de actualización solamente puede ejecutarse después de que transcurra la cantidad de tiempo especificada una vez que se inicia Kaspersky Endpoint Security.

- Configure la tarea de actualización para que se ejecute con los permisos de una cuenta de usuario diferente.

Adición de un origen de actualizaciones

Para agregar un origen de actualizaciones:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione **Actualización**.
En la parte derecha de la ventana se muestra la Configuración de la actualización de la aplicación.
3. En la sección **Modo de ejecución y origen de actualizaciones**, haga clic en el botón **Origen de actualizaciones**.
Esto abre la pestaña **Origen** en la ventana **Actualización**.
4. En la pestaña **Origen**, haga clic en el botón **Agregar**.
Se abre la ventana **Selec. origen de actualizaciones**.
5. En la ventana **Selec. origen de actualizaciones**, seleccione una carpeta con el paquete de instalación o introduzca la ruta completa al archivo en el campo **Origen**.
6. Haga clic en **Aceptar**.
7. En la ventana **Actualización**, haga clic en **Aceptar**.
8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Selección de la región del servidor de actualización

Para seleccionar la región del servidor de actualización:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione **Actualización**.
En la parte derecha de la ventana se muestra la Configuración de la actualización de la aplicación.
3. En la sección **Modo de ejecución y origen de actualizaciones**, haga clic en el botón **Origen de actualizaciones**.
Esto abre la pestaña **Origen** en la ventana **Actualización**.
4. En la pestaña **Origen**, en la sección **Configuración regional**, elija **Seleccionar de la lista**.
5. En la lista desplegable, seleccione el país más próximo a su ubicación actual.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Configuración de actualización desde una carpeta compartida

Configurar actualizaciones de Kaspersky Endpoint Security desde una carpeta compartida consta de los siguientes pasos:

1. Activar la copia de un paquete de actualización en una carpeta compartida en uno de los equipos de la red de área local.
2. Configurar actualizaciones de Kaspersky Endpoint Security desde la carpeta compartida especificada para el resto de los equipos de la red de área local.

Para activar la copia del paquete de actualización en la carpeta compartida:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione **Actualización**.
En la parte derecha de la ventana se muestra la Configuración de la actualización de la aplicación.
3. En la sección **Avanzado**, seleccione la casilla de verificación **Copiar las actualizaciones en la carpeta**.
4. Especifique la ruta de la carpeta compartida en la que se va a colocar el paquete de actualización. Puede hacerlo de una de las siguientes formas:
 - Introduzca la ruta de la carpeta compartida en el campo bajo la casilla de verificación **Copiar las actualizaciones en la carpeta**.
 - Haga clic en el botón **Examinar**. A continuación, en la ventana **Seleccionar carpeta** que se abre, seleccione la carpeta necesaria y haga clic en **Aceptar**.
5. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Para configurar la actualización de Kaspersky Endpoint Security desde una carpeta compartida:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione **Actualización**.
En la parte derecha de la ventana se muestra la Configuración de la actualización de la aplicación.
3. En la sección **Modo de ejecución y origen de actualizaciones**, haga clic en el botón **Origen de actualizaciones**.
Esto abre la pestaña **Origen** en la ventana **Actualización**.
4. En la pestaña **Origen**, haga clic en el botón **Agregar**.
Se abre la ventana **Selec. origen de actualizaciones**.
5. En la ventana **Selec. origen de actualizaciones**, seleccione la carpeta compartida que contiene el paquete de actualización o introduzca la ruta completa de la carpeta compartida en el campo **Origen**.

6. Haga clic en **Aceptar**.
7. En la pestaña **Origen**, desactive la casilla de verificación situada junto a los nombres de los orígenes de actualizaciones que no ha especificado como la carpeta compartida.
8. Haga clic en **Aceptar**.
9. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Selección del modo de ejecución de la tarea de actualización

Para seleccionar el modo de ejecución de la tarea de actualización:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione **Actualización**.
En la parte derecha de la ventana se muestra la Configuración de la actualización de la aplicación.
3. Haga clic en el botón **Modo de ejecución**.
Se abre la pestaña **Modo de ejecución** en la ventana **Actualización**.
4. En la sección **Modo de ejecución**, seleccione una de las siguientes opciones para iniciar una tarea de actualización:
 - Si quiere que Kaspersky Endpoint Security ejecute la tarea de actualización en función de si hay o no disponible un paquete de actualización en el origen de actualizaciones, seleccione **Automático**. La frecuencia de las comprobaciones que realiza Kaspersky Endpoint Security para ver si hay paquetes de actualización aumenta durante los brotes de virus y disminuye en otros momentos.
 - Si quiere iniciar una tarea de actualización manualmente, seleccione **Manual**.
 - Si quiere configurar una planificación de inicio de la tarea de actualización, seleccione **Mediante planificación**.
5. Realice una de las siguientes acciones:
 - Si seleccionó la opción **Automático** o **Manual**, vaya al paso 6 de las instrucciones.
 - Si seleccionó la opción **Mediante planificación**, especifique los parámetros de la planificación de la ejecución de la tarea de actualización. Para ello:
 - a. En la lista desplegable **Frecuencia**, especifique cuándo debe iniciar la tarea de actualización. Seleccione una de las siguientes opciones: **Minutos**, **Horas**, **Días**, **Cada semana**, **A la hora especificada**, **Cada mes** o **Después de iniciar la aplicación**.
 - b. Dependiendo del elemento seleccionado en la lista desplegable **Frecuencia**, especifique los valores de los parámetros que definen el momento del inicio de la tarea de actualización.
 - c. En el campo **Posponer ejecución después del inicio de la aplicación durante**, especifique el intervalo de tiempo que se pospondrá el inicio de la tarea de actualización después del inicio de Kaspersky Endpoint Security.

Si se selecciona el elemento **Después de iniciar la aplicación** en la lista desplegable **Frecuencia**, el campo **Posponer ejecución después del inicio de la aplicación durante** no está disponible.

- d. Si quiere que Kaspersky Endpoint Security ejecute tareas de actualización omitidas en cuanto sea posible, seleccione la casilla de verificación **Ejecutar tareas ignoradas**.

Si se selecciona **Horas**, **Minutos** o **Después de iniciar la aplicación** en la lista desplegable **Frecuencia**, la casilla de verificación **Ejecutar tareas ignoradas** ya no está disponible.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Inicio de una tarea de actualización con los permisos de una cuenta de usuario distinta

De forma predeterminada, la tarea de actualización de Kaspersky Endpoint Security se inicia en nombre del usuario cuya cuenta se ha utilizado para iniciar la sesión en el sistema operativo. Sin embargo, Kaspersky Endpoint Security se puede actualizar desde un origen de actualizaciones al que el usuario no puede acceder debido a la falta de los permisos necesarios (por ejemplo, desde una carpeta compartida que contiene un paquete de actualización) o a no disponer de los permisos de un usuario del servidor proxy autorizado. En la configuración de Kaspersky Endpoint Security, puede especificar un usuario que tenga esos permisos e iniciar la tarea de actualización de Kaspersky Endpoint Security con la cuenta de ese usuario.

Para iniciar una tarea de actualización con una cuenta de usuario distinta:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione **Actualización**.
En la parte derecha de la ventana se muestra la Configuración de la actualización de la aplicación.
3. En la sección **Modo de ejecución y origen de actualizaciones**, haga clic en el botón **Modo de ejecución**.
Se abre la pestaña **Modo de ejecución** en la ventana **Actualización**.
4. En la pestaña **Modo de ejecución**, en la sección **Usuario**, seleccione la casilla de verificación **Ejecutar la tarea como**.
5. En el campo **Nombre**, introduzca el nombre de la cuenta del usuario cuyos derechos sean necesarios para acceder al origen de actualizaciones.
6. En el campo **Contraseña**, introduzca la contraseña del usuario cuyos derechos sean necesarios para acceder al origen de actualizaciones.
7. Haga clic en **Aceptar**.
8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Configurar las actualizaciones de los módulos de la aplicación

Para configurar las actualizaciones de los módulos de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione **Actualización**.
En la parte derecha de la ventana se muestra la Configuración de la actualización de la aplicación.
3. En la sección **Avanzado**, realice una de las siguientes acciones:
 - Seleccione la casilla de verificación **Descargar actualizaciones de los módulos de la aplicación** si desea que la aplicación incluya actualizaciones de los módulos de la aplicación en los paquetes de actualización.
 - Si no, desactive la casilla de verificación **Descargar actualizaciones de los módulos de la aplicación**.
4. Si la casilla de verificación **Descargar actualizaciones de los módulos de la aplicación** se seleccionó en el paso anterior, especifique las condiciones en virtud de las cuales la aplicación instalará las actualizaciones del módulo de la aplicación:
 - Seleccione la opción **Instalar actualizaciones críticas y aprobadas** si desea que la aplicación instale actualizaciones críticas de módulos de la aplicación automáticamente, así como otras actualizaciones después de que se apruebe su instalación, de forma local a través de la interfaz de la aplicación o por parte de Kaspersky Security Center.
 - Seleccione la opción **Instalar solo actualizaciones aprobadas** si desea que la aplicación instale actualizaciones de módulos de la aplicación después de que se apruebe su instalación, de forma local a través de la interfaz de la aplicación o de Kaspersky Security Center.
5. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Inicio y parada de una tarea de actualización

Independientemente del modo de ejecución de la tarea de actualización seleccionado, puede iniciar o parar una tarea de actualización de Kaspersky Endpoint Security en cualquier momento.

Para descargar un paquete de actualización desde los servidores de Kaspersky, se requiere conexión a Internet.

Para iniciar o parar una tarea de actualización:

1. Abra la ventana principal de la aplicación.
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Tareas**.
Se abre la sección **Tareas**.

4. Haga clic con el botón derecho para que aparezca el menú contextual de la línea con el nombre de la tarea de actualización.

Al hacer clic en esta línea, se abre un menú de acciones que se pueden realizar en la tarea de actualización.

5. Realice una de las siguientes acciones:

- Si desea iniciar la tarea de actualización, seleccione **Iniciar la actualización** en el menú.

El estado del progreso de la tarea de actualización, que se muestra a la derecha del botón **Actualización**, cambia a *En ejecución*.

- Si desea parar la tarea de actualización, seleccione **Detener actualización** en el menú.

El estado del progreso de la tarea de actualización, que se muestra a la derecha del botón **Actualización**, cambia a *Parado*.

Anulación de la última actualización

Una vez actualizados las bases de datos y los módulos de la aplicación por primera vez, la función de deshacer la actualización de las bases de datos y los módulos de la aplicación a sus versiones anteriores pasa a estar disponible.

Cada vez que un usuario inicia el proceso de actualización, Kaspersky Endpoint Security crea una copia de respaldo de las bases de datos y de los módulos de la aplicación actuales. Esto permite deshacer la actualización de las bases de datos y de los módulos de la aplicación y restablecer sus versiones anteriores cuando sea necesario. Anular la última actualización es útil, por ejemplo, si la nueva versión de la base de datos contiene una firma no válida que provoca que Kaspersky Endpoint Security bloquee una aplicación segura.

Para anular la última actualización:

1. Abra la ventana principal de la aplicación.

2. Seleccione la pestaña **Protección y control**.

3. Haga clic en la sección **Tareas**.

Se abre la sección **Tareas**.

4. Haga clic con el botón derecho para acceder al menú contextual de la tarea **Actualización**.

5. Seleccione **Deshacer actualización**.

Configuración de los parámetros del servidor proxy

Para configurar el servidor proxy:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione **Actualización**.

En la parte derecha de la ventana se muestra la Configuración de la actualización de la aplicación.

3. En la sección **Servidor proxy**, haga clic en el botón **Configuración**.

Se abre la ventana **Configuración del servidor proxy**.

4. En la ventana **Configuración del servidor proxy**, seleccione la casilla de verificación **Usar servidor proxy**.
5. Especifique la configuración del servidor proxy.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

También puede configurar los parámetros del servidor proxy en la ventana principal de la aplicación, en la pestaña **Configuración**, en la sección **Configuración avanzada**.

Análisis del equipo

Un análisis antivirus es fundamental para la seguridad del equipo. Realice análisis antivirus de forma periódica para ayudar a descartar la posibilidad de que se extienda el software malicioso (malware) que los componentes de protección no han detectado debido a una configuración de nivel de seguridad baja o a otros motivos.

Esta sección describe los detalles y la configuración de las tareas de análisis, los niveles de seguridad, los métodos de análisis y las tecnologías, y ofrece instrucciones sobre la gestión de archivos que Kaspersky Endpoint Security no ha procesado durante el análisis antivirus.

Acerca de las tareas de análisis

Para encontrar virus y otros tipos de software malintencionado (malware) y comprobar la integridad de los módulos de las aplicaciones, Kaspersky Endpoint Security incluye las siguientes tareas:

- **Análisis completo.** Análisis en profundidad de todo el equipo. De forma predeterminada, Kaspersky Endpoint Security analiza los siguientes objetos:
 - Memoria del núcleo
 - Objetos cargados en el inicio del sistema operativo
 - Sectores de arranque
 - Respaldo del sistema operativo
 - Todas las unidades de disco duro y unidades extraíbles
- **Análisis de áreas críticas.** De forma predeterminada, Kaspersky Endpoint Security analiza la memoria del núcleo, ejecutando procesos, y los sectores de arranque del disco.
- **Análisis personalizado.** Kaspersky Endpoint Security analiza los objetos seleccionados por el usuario. Puede analizar cualquier objeto de la siguiente lista:
 - Memoria del núcleo
 - Objetos cargados en el inicio del sistema operativo
 - Respaldo del sistema operativo
 - Buzón de correo de Outlook
 - Todas las unidades de disco duro, unidades extraíbles y unidades de red
 - Cualquier archivo seleccionado
- **Comprobación de integridad.** Kaspersky Endpoint Security realiza una comprobación de los módulos de la aplicación en busca de datos corruptos o modificaciones.

Las tareas Análisis completo y Análisis de áreas críticas son en cierto modo distintas a las demás. Para ellas, no se recomienda editar la cobertura del análisis.

[Después de que comiencen las tareas de análisis](#), se muestra el progreso en el campo que hay junto al nombre de la tarea de análisis en ejecución, en la sección **Tareas** de la pestaña **Protección y control** de la ventana principal de Kaspersky Endpoint Security.

La información sobre los resultados del análisis y los eventos que se han producido durante la ejecución de las tareas de análisis se registran en un informe de Kaspersky Endpoint Security.

Inicio o detención de una tarea de análisis

Con independencia del modo de ejecución de la tarea de análisis seleccionado, puede iniciar o parar una tarea de análisis en cualquier momento.

Para iniciar o parar una tarea de análisis:

1. Abra la [ventana principal de la aplicación](#).
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Tareas**.
Se abre la sección **Tareas**.
4. Haga clic con el botón derecho para que aparezca el menú contextual de la línea con el nombre de la tarea de análisis.
Se abre un menú con las acciones de la tarea de análisis.
5. Realice una de las siguientes acciones:
 - Si desea iniciar la tarea de análisis, seleccione **Iniciar análisis** en el menú.
El estado del progreso de la tarea que se muestra a la derecha del botón con el nombre de esta tarea cambia a *En ejecución*.
 - Si desea parar la tarea de análisis, seleccione **Detener análisis** en el menú.
El estado del progreso de la tarea que se muestra a la derecha del botón con el nombre de esta tarea cambia a *Detenido*.

Configuración de los parámetros de las tareas de análisis

Para configurar los parámetros de las tareas de análisis puede llevar a cabo los siguientes pasos:

- Modificar el nivel de seguridad.
Puede seleccionar uno de los niveles de seguridad predeterminados o ajustar manualmente la configuración del nivel de seguridad. Si cambia la configuración del nivel de seguridad, siempre puede volver a la configuración recomendada del nivel de seguridad.
- Modifique la acción que realizará Kaspersky Endpoint Security en el caso de que detecte un archivo infectado.
- Modifique la cobertura del análisis.
Puede ampliar o reducir la cobertura del análisis si agrega o elimina objetos para el análisis, o si cambia el tipo de los archivos que deben analizarse.

- Optimice el análisis.

Puede optimizar el análisis de archivos: reduzca el tiempo de análisis y aumente la velocidad de funcionamiento de Kaspersky Endpoint Security. Esto se puede conseguir si analiza solamente los archivos nuevos y los que se hayan modificado desde el último análisis. Este modo se aplica tanto a archivos simples como a compuestos. También puede establecer un límite para la duración del análisis de un único archivo. Cuando se supera el intervalo de tiempo especificado, Kaspersky Endpoint Security excluye el archivo del análisis actual (excepto los archivos y objetos que incluyen varios archivos).

También puede activar el uso de las tecnologías iChecker e iSwift. Estas tecnologías optimizan la velocidad del análisis de archivos ya que excluyen archivos que no han sido modificados desde el análisis más reciente.

- Configurar el análisis de archivos compuestos.

- Configure el uso de métodos de análisis.

Cuando está activo, Kaspersky Endpoint Security utiliza el análisis de firmas. Durante el análisis de firmas, Kaspersky Endpoint Security equipara el objeto detectado con los registros en su base de datos. Siguiendo las recomendaciones de los expertos de Kaspersky, el análisis de firmas está siempre activado.

Para aumentar la eficacia de la protección, puede usar el análisis heurístico. Durante el análisis heurístico, Kaspersky Endpoint Security analiza la actividad de objetos en el sistema operativo. El análisis heurístico puede detectar objetos maliciosos para los que no existen registros actualmente en la base de datos de Kaspersky Endpoint Security.

- Seleccione el modo de ejecución de la tarea de análisis.

Si no es posible iniciar la tarea de análisis por alguna razón (por ejemplo, el equipo estaba apagado en ese momento), puede configurar la tarea que se ha omitido para que se inicie automáticamente lo antes posible.

Puede retrasar la ejecución de la tarea de análisis después de que la aplicación se inicie si ha seleccionado el modo de ejecución de la tarea de actualización **Mediante planificación** y si el momento del inicio de Kaspersky Endpoint Security coincide con la planificación de la ejecución de la tarea de análisis. La tarea de análisis solo puede ejecutarse después de que transcurra el intervalo de tiempo especificado una vez que se inicie Kaspersky Endpoint Security.

- Configure la tarea de análisis para que se ejecute con una cuenta de usuario distinta.

- Especifique la configuración para el análisis de unidades extraíbles cuando se conectan.

Cambiar el nivel de seguridad

Kaspersky Endpoint Security utiliza varias combinaciones de parámetros para realizar las tareas de análisis. Estas combinaciones de ajustes guardados en la aplicación se denominan *niveles de seguridad*. Existen tres niveles de seguridad predeterminados: **Máximo**, **Recomendado** y **Mínimo**. La configuración del nivel de seguridad **Recomendado** se considera óptima. Los expertos de Kaspersky la recomiendan.

Para cambiar un nivel de seguridad:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione el apartado que contenga el nombre de la tarea de análisis requerida (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).

En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.

3. En la sección **Nivel de seguridad**, lleve a cabo una de las siguientes acciones:

- Si desea aplicar uno de los niveles de seguridad predeterminados (**Máximo**, **Recomendado** o **Mínimo**), selecciónelo con el control deslizante.
- Si desea configurar un nivel de seguridad personalizado, haga clic en el botón **Configuración** y, en la ventana que aparece, especifique la configuración con el nombre de una tarea de análisis.
Después de configurar un nivel de seguridad personalizado, el nombre del nivel de seguridad de la sección **Nivel de seguridad** cambia a **Personalizado**.
- Si desea cambiar el nivel de seguridad a **Recomendado**, haga clic en el botón **Predeterminado**.

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Modificación de las acciones que se van a realizar en archivos infectados

Para cambiar la acción que se debe realizar con los archivos infectados:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione el apartado que contenga el nombre de la tarea de análisis requerida (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).

En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.

3. En la sección **Acción al detectar una amenaza**, seleccione la opción requerida:

- **Seleccionar la acción automáticamente.**
- **Realizar acción.**

4. Si seleccionó la opción **Realizar acción** durante el paso anterior, seleccione las siguientes casillas de verificación:

- Seleccione la casilla de verificación **Desinfectar** si desea que Kaspersky Endpoint Security desinfecte los objetos en los que se hayan detectado amenazas.

Incluso si se selecciona esta opción, Kaspersky Endpoint Security aplica la acción **Eliminar** a los archivos que forman parte de la aplicación Tienda Windows.

- Seleccione la casilla de verificación **Eliminar** si desea que Kaspersky Endpoint Security los objetos en los que se hayan detectado amenazas.
- Seleccione las casillas de verificación **Desinfectar** y **Eliminar** si desea que Kaspersky Endpoint Security trate de desinfectar los objetos en los que se detecten amenazas y elimine aquellos objetos que no se puedan desinfectar.
- Desactive las casillas de verificación **Desinfectar** y **Eliminar** si desea que Kaspersky Endpoint Security no tome ninguna medida sobre los objetos en los que se detectan amenazas, sino que, en lugar de eso, simplemente notifique al usuario acerca de los resultados del análisis de dichos objetos.

5. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Generación de una lista de objetos para analizar

Para generar una lista de objetos para analizar, puede usar uno de los dos métodos siguientes:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

Este método solo está disponible para las tareas **Análisis completo** y **Análisis de áreas críticas**. La lista de objetos que se van a analizar para la tarea **Análisis personalizado** solo se puede crear en la pestaña **Protección y control**.

*Para crear una lista de objetos para analizar en la pestaña **Protección y control** de la ventana principal de la aplicación:*

1. Abra la ventana principal de la aplicación.
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Tareas**.
Se abre la sección **Tareas**.
4. Haga clic con el botón derecho del ratón para abrir el menú contextual de la línea que contiene el nombre de la tarea y seleccione **Cobertura del análisis**.
Se abre la ventana **Cobertura del análisis**.
5. Si desea agregar un nuevo objeto a la cobertura del análisis:
 - a. Haga clic en el botón **Agregar**.
Se abre la ventana **Seleccionar cobertura del análisis**.
 - b. Seleccione el objeto y haga clic en **Agregar**.
Todos los objetos seleccionados en la ventana **Seleccionar cobertura del análisis** se muestran en la lista **Cobertura del análisis**.
 - c. Haga clic en **Aceptar**.
6. Si desea cambiar la ruta a un objeto incluido en la cobertura del análisis:
 - a. Seleccione el objeto incluido en la cobertura del análisis.
 - b. Haga clic en el botón **Modificar**.
Se abre la ventana **Seleccionar cobertura del análisis**.
 - c. Introduzca la nueva ruta al objeto incluido en la cobertura del análisis.
 - d. Haga clic en **Aceptar**.
7. Si desea eliminar un objeto de la cobertura del análisis:

a. Seleccione el objeto que desea eliminar de la cobertura del análisis.

Para seleccionar varios objetos, selecciónelos mientras mantiene pulsada la tecla **CTRL**.

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

Se abre una ventana para que confirme la eliminación.

c. Haga clic en **Sí** en la ventana de confirmación de eliminación.

No puede eliminar ni editar objetos que se incluyan en la cobertura del análisis predeterminada.

8. Para excluir un objeto de la cobertura del análisis, desactive la casilla de verificación que hay junto a los objetos de la lista **Cobertura del análisis**.

El objeto sigue en la lista de objetos de la cobertura del análisis, pero no se analiza cuando se ejecuta la tarea de análisis.

9. Haga clic en **Aceptar**.

10. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Para crear una lista de objetos para analizar desde la ventana de configuración de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione el apartado con el nombre de la tarea de análisis requerida: **Análisis completo** o **Análisis de áreas críticas**.

En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.

3. Haga clic en el botón **Cobertura del análisis**.

Se abre la ventana **Cobertura del análisis**.

4. Cree una lista de objetos para analizar según los pasos 5 a 10 de las instrucciones anteriores.

Selección del tipo de archivo que se va a analizar

Puede usar los dos métodos siguientes para seleccionar el tipo de archivo que se va a analizar:

- En la pestaña **Protección y control** de la [ventana principal de la aplicación](#)
- Desde la [ventana de configuración de la aplicación](#)

Este método solo está disponible para las tareas **Análisis completo** y **Análisis de áreas críticas**. El tipo de archivo que se va a analizar con la tarea **Análisis personalizado** solo se puede seleccionar en la pestaña **Protección y control**.

*Para seleccionar el tipo de archivo que se va a analizar en la pestaña **Protección y control** de la ventana principal de la aplicación:*

1. Abra la ventana principal de la aplicación.

2. Seleccione la pestaña **Protección y control**.

3. Haga clic en la sección **Tareas**.

Se abre la sección **Tareas**.

4. Haga clic con el botón derecho del ratón para abrir el menú contextual de la línea que contiene el nombre de la tarea y seleccione **Configuración**.

Se abre una ventana con el nombre de la tarea de análisis seleccionada.

5. En la ventana con el nombre de la tarea de análisis seleccionada, seleccione la pestaña **Cobertura**.

6. En la sección **Tipos de archivos**, especifique el tipo de archivos que desea analizar cuando se ejecute la tarea de análisis seleccionada:

- Si quiere analizar todos los archivos, seleccione **Todos los archivos**.
- Si quiere analizar los archivos con los formatos más vulnerables a los virus, seleccione **Analizar archivos por formato**.
- Si quiere analizar los archivos con las extensiones más vulnerables habitualmente a los virus, seleccione **Analizar archivos por extensión**.

Al seleccionar el tipo de archivos que vayan a analizarse, tenga en cuenta lo siguiente:

- Existen algunos formatos de archivo (como TXT) para los que hay una baja probabilidad de intrusión de código malicioso y su posterior activación. De igual modo, otros formatos de archivos contienen o pueden contener código ejecutable (por ejemplo: .exe, .dll y .doc). Es elevado el riesgo de penetración y activación de código malicioso en estos archivos.
- Un intruso puede enviar un virus u otro programa malicioso a su equipo en un archivo ejecutable al que se ha cambiado el nombre con la extensión .txt. Si selecciona el análisis de archivos por extensión, la aplicación omitirá el archivo durante el análisis. Si se selecciona el análisis de archivos por formato, Antivirus de archivos analiza el encabezado del archivo sin tener en cuenta la extensión. Si este análisis revela que el archivo tiene el formato EXE, la aplicación lo analiza.

7. En la ventana que contiene el nombre de una tarea de análisis, haga clic en **Aceptar**.

8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Para seleccionar el tipo de archivo que se va a analizar desde la ventana de configuración de la aplicación:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione el apartado con el nombre de la tarea de análisis requerida: **Análisis completo** o **Análisis de áreas críticas**.

En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.

3. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.

Se abre una ventana con el nombre de la tarea de análisis seleccionada.

4. En la ventana con el nombre de la tarea de análisis seleccionada, seleccione la pestaña **Cobertura**.

5. Complete los pasos 5 a 7 de las instrucciones anteriores.

Optimización del análisis de archivos

Para optimizar el análisis de archivos:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione el apartado que contenga el nombre de la tarea de análisis requerida (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).
En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.
3. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
Se abre una ventana con el nombre de la tarea de análisis seleccionada.
4. En la ventana de diálogo que se abre, seleccione la pestaña **Cobertura**.
5. En la sección **Optimización del análisis**, lleve a cabo las siguientes acciones:
 - Seleccione la casilla de verificación **Analizar solamente archivos nuevos y modificados**.
 - Seleccione la casilla de verificación **Omitir archivos analizados un máximo de** y especifique la duración del análisis de un único archivo (en segundos).
6. Haga clic en **Aceptar**.
7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Análisis de archivos compuestos

Una técnica común para ocultar virus y otro tipo de software malicioso (malware) consiste en implantarlos en archivos compuestos, como archivos comprimidos o bases de datos. Para detectar virus y otro tipo de software malicioso (malware) oculto de este modo, se debe descomprimir el archivo compuesto, lo que puede ralentizar el análisis. Puede limitar los tipos de archivos compuestos que se deben analizar, lo que permite acelerar el análisis.

Para configurar el análisis de archivos compuestos:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione el apartado que contenga el nombre de la tarea de análisis requerida (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).
En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.
3. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
Se abre una ventana con el nombre de la tarea de análisis seleccionada.
4. En la ventana de diálogo que se abre, seleccione la pestaña **Cobertura**.

5. En la sección **Análisis de archivos compuestos**, especifique qué archivos compuestos desea analizar: archivos comprimidos, paquetes de instalación, archivos en formatos de Office, archivos de formato de correo o archivos protegidos con contraseña.
6. Si la casilla de verificación **Analizar solamente archivos nuevos y modificados** está desactivada en la sección **Optimización del análisis**, haga clic en el enlace **todos/nuevos** situado junto al nombre del tipo de archivo compuesto si desea especificar, para cada tipo de archivo compuesto, si se analizan todos los archivos de dicho tipo o solo los nuevos.
Al hacer clic en este enlace, cambia su valor.
Si se selecciona la casilla de verificación **Analizar solamente archivos nuevos y modificados**, solo se analizarán los archivos nuevos.
7. Haga clic en el botón **Avanzado**.
Se abre la ventana **Archivos compuestos**.
8. En la sección **Límite de tamaño**, lleve a cabo una de las siguientes acciones:
 - Si no quiere descomprimir archivos compuestos de gran tamaño, seleccione la casilla de verificación **No descomprimir archivos compuestos de gran tamaño** y especifique el valor requerido en el campo **Tamaño máximo de archivo**.
 - Si quiere descomprimir archivos compuestos con independencia de su tamaño, desactive la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**.

Kaspersky Endpoint Security analiza los archivos de gran tamaño extraídos de archivos comprimidos, con independencia de si se ha seleccionado la casilla de verificación **No descomprimir archivos compuestos de gran tamaño**.

9. Haga clic en **Aceptar**.
10. En la ventana con el nombre de una tarea de análisis, haga clic en el botón **Aceptar**.
11. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Uso de métodos de análisis

Para utilizar métodos de análisis:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione el apartado que contenga el nombre de la tarea de análisis requerida (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).
En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.
3. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
Se abre una ventana con el nombre de la tarea de análisis seleccionada.
4. En la ventana que aparece, seleccione la pestaña **Avanzado**.

5. Si desea que la aplicación lleve a cabo un análisis heurístico cuando ejecute una tarea de análisis, en la sección **Métodos de análisis**, active la casilla de verificación **Análisis heurístico**. A continuación, utilice el control deslizante para definir el análisis de nivel heurístico: **Análisis superficial**, **Análisis medio** o **Análisis avanzado**.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Uso de tecnologías de análisis

Para utilizar tecnologías de análisis:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione el apartado que contenga el nombre de la tarea de análisis requerida (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).
En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.
3. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
Se abre una ventana con el nombre de la tarea de análisis seleccionada.
4. En la ventana que aparece, seleccione la pestaña **Avanzado**.
5. En la sección **Tecnologías de análisis**, seleccione las casillas de verificación que hay junto a los nombres de las tecnologías que quiere utilizar durante el análisis.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Seleccionar el modo de ejecución para la tarea de análisis

Para seleccionar el modo de ejecución de la tarea de análisis:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione el apartado que contenga el nombre de la tarea requerida (**Análisis completo**, **Análisis de áreas críticas** o **Análisis personalizado**).
En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.
3. Haga clic en el botón **Modo de ejecución**.
Se abre una ventana con las propiedades de la tarea seleccionada en la pestaña **Modo de ejecución**.
4. En la sección **Modo de ejecución**, seleccione el modo de ejecución de la tarea: **Manual** o **Mediante planificación**.
5. Si seleccionó la opción **Mediante planificación**, especifique los ajustes de la planificación. Para ello:

- a. En la lista desplegable **Frecuencia**, seleccione la frecuencia de ejecución de la tarea (**Minutos, Horas, Días, Cada semana, A la hora especificada, Cada mes, Después de iniciar la aplicación o Después de cada actualización**).
- b. Según la frecuencia seleccionada, configure los ajustes avanzados que especifican la planificación de la ejecución de la tarea.
- c. Si quiere que Kaspersky Endpoint Security ejecute tareas de análisis ignoradas lo antes posible, seleccione la casilla de verificación **Ejecutar tareas ignoradas**.

Si selecciona los elementos **Minutos, Horas, Después de iniciar la aplicación o Después de cada actualización** en la lista desplegable **Frecuencia**, la casilla de verificación **Ejecutar tareas ignoradas** dejará de estar disponible.

- a. Si desea que Kaspersky Endpoint Security suspenda una tarea cuando los recursos informáticos sean limitados, seleccione la casilla de verificación **Ejecutar solo cuando el equipo está inactivo**.

Esta opción de planificación ayuda a ahorrar recursos del equipo.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Inicio de una tarea de análisis con la cuenta de un usuario distinto

De forma predeterminada, una tarea de análisis se realiza con los permisos de la cuenta con la que el usuario ha iniciado sesión en el sistema operativo. Sin embargo, cabe la posibilidad de que necesite ejecutar una tarea de análisis con una cuenta distinta. Puede especificar un usuario que tenga los permisos adecuados en la configuración de tarea de análisis y realizar la tarea de análisis con esta cuenta de usuario.

Para configurar el inicio de una tarea de análisis con una cuenta de usuario distinta:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione el apartado que contenga el nombre de la tarea requerida (**Análisis completo, Análisis de áreas críticas o Análisis personalizado**).
En la parte derecha de la ventana, se muestra la configuración de la tarea de análisis seleccionada.
3. Haga clic en el botón **Modo de ejecución**.
Esto abre una ventana con las propiedades de la tarea seleccionada en la pestaña **Modo de ejecución**.
4. En la pestaña **Modo de ejecución**, en la sección **Usuario**, seleccione la casilla de verificación **Ejecutar la tarea como**.
5. En el campo **Nombre**, introduzca el nombre de la cuenta del usuario cuyos derechos sean necesarios para iniciar la tarea de análisis.
6. En el campo **Contraseña**, introduzca la contraseña del usuario cuyos derechos sean necesarios para iniciar la tarea de análisis.
7. Haga clic en **Aceptar**.
8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Análisis de unidades extraíbles cuando se conectan al equipo

Algunos programas maliciosos explotan las vulnerabilidades del sistema operativo para reproducirse mediante redes locales y unidades extraíbles. Kaspersky Endpoint Security le permite analizar unidades extraíbles que se conectan a su equipo en busca de virus y otro software malicioso (malware).

Para configurar el análisis de unidades extraíbles cuando se conectan:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, seleccione la sección **Tareas planificadas**.

La configuración de tareas se muestra en la parte derecha de la ventana.

3. En la sección **Analizar las unidades extraíbles al conectarlas**, seleccione la acción requerida en la lista desplegable **Acción al conectar una unidad extraíble**:

- **No analizar**

- **Análisis detallado**

En este modo, Kaspersky Endpoint Security analiza todos los archivos ubicados en la unidad extraíble, incluidos los archivos que hay dentro de objetos compuestos.

- **Análisis rápido**

En este modo, Kaspersky Endpoint Security analiza solo los [archivos potencialmente](#) infectables y no descomprime objetos compuestos.

4. Si desea que Kaspersky Endpoint Security analice únicamente aquellas unidades extraíbles cuyo tamaño sea igual o menor al valor especificado, seleccione la casilla de verificación **Tamaño máximo de la unidad extraíble** y especifique un valor en megabytes en el campo adyacente.

5. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Gestión de archivos sin procesar

Esta sección contiene instrucciones sobre la gestión de archivos infectados o probablemente infectados que Kaspersky Endpoint Security no ha procesado mientras realizaba el análisis del equipo en busca de virus y otras amenazas.

Acerca de los archivos sin procesar

Kaspersky Endpoint Security registra información sobre los archivos que no ha procesado por alguna razón. Esta información se recoge como eventos en la lista de archivos sin procesar.

Un archivo infectado se considera *procesado* si Kaspersky Endpoint Security lleva a cabo una de las siguientes acciones en el archivo de acuerdo con la configuración especificada de la aplicación mientras analiza el equipo en busca de virus y otras amenazas:

- Desinfectar.

- Eliminar.
- Eliminar si falla la desinfección.

Un archivo infectado se considera *no procesado* si, por cualquier motivo, Kaspersky Endpoint Security no lleva a cabo una acción en el archivo de acuerdo con la configuración especificada de la aplicación mientras analiza el equipo en busca de virus y otras amenazas.

Esta situación puede darse en los siguientes casos:

- El archivo analizado no está disponible (por ejemplo, se encuentra en una unidad de red o en una unidad extraíble sin derechos de escritura).
- La acción seleccionada para analizar tareas en la sección **Acción al detectar una amenaza** es **Informar** y, cuando aparece una notificación sobre el archivo infectado, el usuario selecciona la acción **Omitir**.

Puede iniciar manualmente una tarea de análisis personalizado para archivos de la lista de archivos sin procesar después de actualizar las bases de datos y los módulos de aplicación. El estado del archivo puede variar tras el análisis. Puede llevar a cabo las acciones necesarias en los archivos, en función de su estado.

Por ejemplo, puede llevar a cabo las siguientes acciones:

- [Eliminar archivos con el estado *Infectado*](#).
- Restaurar archivos infectados que contengan información importante y *restablecer archivos marcados como Desinfectado* o como No infectado.
- Archivos en cuarentena con el estado *Probablemente infectado*.

Gestión de la lista de archivos sin procesar

La lista de archivos sin procesar aparece en forma de una tabla.

Puede realizar las siguientes operaciones con archivos sin procesar:

- Ver la lista de archivos sin procesar.
- Analizar los archivos sin procesar utilizando la versión actual de las bases de datos y los módulos de Kaspersky Endpoint Security.
- Restaurar los archivos de la lista de archivos sin procesar en las carpetas originales o en una carpeta distinta de su elección (cuando no se puede escribir en la carpeta original).
- Quite archivos de la lista de archivos sin procesar.
- Abrir la carpeta en la que se encontraba originalmente el archivo sin procesar.

También puede llevar a cabo las siguientes acciones mientras gestiona los datos de la tabla:

- Filtrar eventos de archivos no procesados por condiciones de filtro personalizadas o valores de columnas.
- Usar la función de búsqueda de eventos de archivos sin procesar.
- Ordenar eventos de archivos sin procesar.

- Cambiar el orden y el conjunto de columnas que se muestran en la lista de archivos sin procesar.
- Agrupar eventos de archivos sin procesar.

Puede copiar los eventos de los archivos sin procesar seleccionados en el portapapeles, si fuera necesario.

Inicio de una tarea de análisis personalizado para archivos sin procesar

Puede iniciar manualmente una tarea de análisis personalizado de archivos sin procesar. Puede iniciar el análisis si, por ejemplo, el último análisis se interrumpió por algún motivo o si desea volver a analizar archivos sin procesar tras la última actualización de las bases de datos y módulos de la aplicación.

Para ejecutar un análisis personalizado de archivos sin procesar, haga lo siguiente:

1. Abra la [ventana principal de la aplicación](#).
2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Cuarentena** para abrir la ventana **Almacenes**.
3. En la ventana **Almacenes**, seleccione la pestaña **Archivos sin procesar**.
4. En la tabla de la pestaña **Archivos sin procesar**, seleccione uno o varios eventos asociados a los archivos que desee analizar.
Para seleccionar varios eventos, selecciónelos manteniendo pulsada la tecla **CTRL**.
5. Inicie la tarea Análisis personalizado de una de las siguientes formas:
 - Haga clic en el botón **Volver a analizar**.
 - Haga clic con el botón derecho para que aparezca el menú contextual y seleccione **Volver a analizar**.

Eliminación de archivos de la lista de archivos sin procesar

Para eliminar los archivos de la lista de archivos sin procesar, haga lo siguiente:

1. Abra la [ventana principal de la aplicación](#).
2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Cuarentena** para abrir la ventana **Almacenes**.
3. En la ventana **Almacenes**, seleccione la pestaña **Archivos sin procesar**.
4. En la tabla de la pestaña **Archivos sin procesar**, seleccione uno o varios eventos asociados con los archivos que desee eliminar.
Para seleccionar varios eventos, selecciónelos manteniendo pulsada la tecla **CTRL**.
5. Elimine archivos de uno de los siguientes modos:
 - Haga clic en el botón **Eliminar**.

- Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Eliminar**.

Análisis de vulnerabilidades

Esta sección contiene información sobre los detalles y la configuración de la tarea Análisis de vulnerabilidades, así como instrucciones sobre la gestión de la lista de vulnerabilidades detectadas por Kaspersky Endpoint Security durante la ejecución de la tarea Análisis de vulnerabilidades.

Visualización de información sobre vulnerabilidades de aplicaciones en ejecución

La información sobre vulnerabilidades de aplicaciones en ejecución está disponible si Kaspersky Endpoint Security se instala en un equipo que ejecuta Microsoft Windows para estaciones de trabajo. Esta información no está disponible si Kaspersky Endpoint Security se instala en un equipo con [Microsoft Windows para servidores de archivos](#).

Para ver información sobre vulnerabilidades de aplicaciones en ejecución:

1. Abra la [ventana principal de la aplicación](#).
2. Seleccione la pestaña **Protección y control**.
3. Se abre la sección **Control de Endpoint**.
4. Haga clic en el botón **Supervisión de la actividad de aplicaciones**.

La ventana **Control de actividad de aplicaciones** se abre en la pestaña **Supervisión de la actividad de aplicaciones**. La tabla **Supervisión de la actividad de aplicaciones** muestra información resumida sobre la actividad de las aplicaciones en ejecución en el sistema operativo. La gravedad de vulnerabilidad de las aplicaciones en ejecución, según determina el componente Control de vulnerabilidades, se muestra en la columna **Estado de vulnerabilidad**.

Acerca de la tarea Análisis de vulnerabilidades

Las vulnerabilidades del sistema operativo pueden deberse, por ejemplo, a errores de programación o diseño, contraseñas poco seguras o actividad de software malicioso (malware). Cuando se realiza un análisis en busca de vulnerabilidades, la aplicación analiza el sistema operativo y busca anomalías y parámetros dañados de aplicaciones de Microsoft y otros proveedores.

El análisis de vulnerabilidades realiza el diagnóstico de seguridad del sistema operativo y detecta las características de software que los intrusos pueden usar para propagar objetos maliciosos y obtener acceso a la información personal.

Una vez que [se inicia la tarea Análisis de vulnerabilidades](#), se muestra su progreso en el campo situado junto al nombre de la tarea **Análisis de vulnerabilidades** de la sección **Tareas**, en la pestaña **Protección y control** de la ventana principal de Kaspersky Endpoint Security.

Los resultados de la tarea Análisis de vulnerabilidades se registran en [informes](#).

Inicio o detención de la tarea Análisis de vulnerabilidades

Independientemente del modo de ejecución que se seleccione para la tarea Análisis de vulnerabilidades, puede ejecutarla o detenerla en cualquier momento.

Para ejecutar o detener la tarea Análisis de vulnerabilidades, haga lo siguiente:

1. Abra la [ventana principal de la aplicación](#).
2. Seleccione la pestaña **Protección y control**.
3. Haga clic en la sección **Tareas**.
Se abre la sección **Tareas**.
4. Haga clic con el botón derecho para que aparezca el menú contextual de la línea con el nombre de la tarea Análisis de vulnerabilidades.
Se abre un menú de las operaciones de la tarea Análisis de vulnerabilidades.
5. Realice una de las siguientes acciones:
 - Para ejecutar la tarea Análisis de vulnerabilidades, seleccione **Iniciar análisis** del menú.
El estado del progreso de la tarea que se muestra a la derecha del botón con el nombre de la tarea Análisis de vulnerabilidades cambia a *En ejecución*.
 - Para detener la tarea Análisis de vulnerabilidades, seleccione **Detener análisis** del menú.
El estado del progreso de la tarea que se muestra a la derecha del botón con el nombre de la tarea Análisis de vulnerabilidades cambia a *Detenido*.

Configurar los ajustes de Análisis de vulnerabilidades

Para configurar los parámetros de Análisis de vulnerabilidades, puede realizar las siguientes acciones:

- Cree la cobertura del análisis de vulnerabilidades.
Puede ampliar o restringir la cobertura del análisis al agregar o al eliminar aplicaciones para que se analicen en busca de vulnerabilidades.
- Seleccione el modo de ejecución para la tarea Análisis de vulnerabilidades.
Si no es posible iniciar la tarea de análisis por alguna razón (por ejemplo, el equipo estaba apagado en ese momento), puede configurar la tarea que se ha omitido para que se ejecute automáticamente lo antes posible.
- Configure la tarea para que se ejecute con los permisos de una cuenta de usuario diferente.
De forma predeterminada, una tarea de análisis se realiza con los permisos de la cuenta con la que el usuario ha iniciado sesión en el sistema operativo. Sin embargo, cabe la posibilidad de que necesite ejecutar una tarea de análisis con una cuenta distinta. Puede especificar un usuario que tenga los permisos adecuados en la configuración de la tarea y ejecutar dicha tarea con esta cuenta de usuario.

Creación de la cobertura del análisis de vulnerabilidades

Una cobertura del análisis de vulnerabilidades es un proveedor de software o una ruta de la carpeta en la que se ha instalado el software (por ejemplo, todas las aplicaciones de Microsoft que se instalan en la carpeta Archivos de programa).

Para crear una cobertura del análisis de vulnerabilidades:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione **Análisis de vulnerabilidades**.
En la parte derecha de la ventana, se muestra la configuración de la tarea Análisis de vulnerabilidades.
3. En la sección **Cobertura del análisis**:
 - a. Para que Kaspersky Endpoint Security busque vulnerabilidades en las aplicaciones de Microsoft instaladas en el equipo, seleccione la casilla de verificación **Microsoft**.
 - b. Para que Kaspersky Endpoint Security busque vulnerabilidades en las aplicaciones instaladas en el equipo que no son de Microsoft, seleccione la casilla de verificación **Otros proveedores**.
 - c. En la ventana **Áreas adicionales de análisis de vulnerabilidades**, haga clic en el botón **Configuración**.
Se abre la ventana **Cobertura del análisis de vulnerabilidades**.
 - d. Cree la cobertura del análisis de vulnerabilidades mediante los botones **Agregar** y **Eliminar**.
 - e. En la ventana **Cobertura del análisis de vulnerabilidades**, haga clic en **Aceptar**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Seleccionar el modo de ejecución para la tarea de Análisis de vulnerabilidades

Para seleccionar el modo de ejecución de la tarea Análisis de vulnerabilidades, haga lo siguiente:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione **Análisis de vulnerabilidades**.
En la parte derecha de la ventana, se muestra la configuración de la tarea Análisis de vulnerabilidades.
3. Haga clic en el botón **Modo de ejecución**.
Esto abre la pestaña **Modo de ejecución** en la ventana **Análisis de vulnerabilidades**.
4. En la sección **Modo de ejecución**, seleccione una de las siguientes opciones de modo de ejecución para iniciar la tarea Análisis de vulnerabilidades:
 - Si quiere iniciar una tarea Análisis de vulnerabilidades manualmente, seleccione **Manual**.

- Si quiere configurar una planificación de inicio de la tarea Análisis de vulnerabilidades, seleccione **Mediante planificación**.

5. Realice una de las siguientes acciones:

- Si selecciona la opción **Manual**, vaya al paso 6 de estas instrucciones.
- Si ha seleccionado la opción **Mediante planificación**, especifique los parámetros de ejecución de la tarea Análisis de vulnerabilidades. Para ello:
 - a. En la lista desplegable **Frecuencia**, especifique cuándo iniciar la tarea Análisis de vulnerabilidades. Seleccione una de las siguientes opciones: **Días**, **Cada semana**, **A la hora especificada**, **Cada mes**, **Después de iniciar la aplicación** o **Después de cada actualización**.
 - b. En función del elemento seleccionado en la lista desplegable **Frecuencia**, especifique los valores de los parámetros que definen el momento del inicio de la tarea Análisis de vulnerabilidades.
 - c. Si quiere que Kaspersky Endpoint Security ejecute tareas de Análisis de vulnerabilidades ignoradas lo antes posible, seleccione la casilla de verificación **Ejecutar tareas ignoradas**.

Si selecciona **Después de iniciar la aplicación** o **Después de cada actualización** en la lista desplegable **Frecuencia**, la casilla de verificación **Ejecutar tareas ignoradas** no está disponible.

6. Haga clic en **Aceptar**.

7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Iniciar una tarea de análisis de vulnerabilidades con los permisos de una cuenta de usuario distinta

De forma predeterminada, la tarea Análisis de vulnerabilidades se ejecuta con la cuenta con la que el usuario ha iniciado sesión en el sistema operativo. Sin embargo, cabe la posibilidad de que necesite ejecutar la tarea Análisis de vulnerabilidades con una cuenta de usuario distinta. Puede especificar un usuario con estos derechos en la configuración de la tarea Análisis de vulnerabilidades e iniciar la tarea Análisis de vulnerabilidades con la cuenta de este usuario.

Para configurar el inicio de la tarea Análisis de vulnerabilidades con una cuenta de usuario diferente, haga lo siguiente:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione **Análisis de vulnerabilidades**. En la parte derecha de la ventana, se muestra la configuración de la tarea Análisis de vulnerabilidades.
3. Haga clic en el botón **Modo de ejecución**. Esto abre la pestaña **Modo de ejecución** en la ventana **Análisis de vulnerabilidades**.
4. En la pestaña **Modo de ejecución**, en la sección **Usuario**, seleccione la casilla de verificación **Ejecutar la tarea como**.
5. En el campo **Nombre**, introduzca el nombre de cuenta del usuario cuyos derechos sean necesarios para iniciar la tarea Análisis de vulnerabilidades.

6. En el campo **Contraseña**, introduzca la contraseña del usuario cuyos derechos sean necesarios para iniciar la tarea Análisis de vulnerabilidades.
7. Haga clic en **Aceptar**.
8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Gestión de la lista de vulnerabilidades

Al gestionar la lista de vulnerabilidades, puede llevar a cabo las siguientes acciones:

- Ver la lista de vulnerabilidades.
- Iniciar de nuevo la tarea Análisis de vulnerabilidades después de actualizar las bases de datos y los módulos de aplicación.
- Ver información detallada acerca de la vulnerabilidad y las recomendaciones sobre su corrección en una sección independiente.
- Ocultar las entradas seleccionadas en la lista de vulnerabilidades.
- Filtrar por nivel de importancia la lista de vulnerabilidades.
- Filtrar la lista de vulnerabilidades por los valores de estado *Arreglado* u *Oculto*.

También puede llevar a cabo las siguientes acciones mientras gestiona los datos de la tabla:

- Filtrar la lista de vulnerabilidades por los valores de columna o por las condiciones de filtrado personalizadas.
- Utilizar la función de búsqueda de vulnerabilidades.
- Ordenar entradas en la lista de vulnerabilidades.
- Cambiar el orden y la distribución de las columnas que se muestran en la lista de vulnerabilidades.
- Agrupar entradas en la lista de vulnerabilidades.

Acerca de la lista de vulnerabilidades

Kaspersky Endpoint Security registra los resultados de la [tarea Análisis de vulnerabilidades](#) en la lista de vulnerabilidades.

Después de que se revisen las vulnerabilidades seleccionadas y se realicen las acciones recomendadas para corregirlas, Kaspersky Endpoint Security cambia el estado de las vulnerabilidades a *Arreglado*.

Si no quiere mostrar las entradas sobre vulnerabilidades específicas en la lista de vulnerabilidades, puede elegir ocultar estas entradas. Kaspersky Endpoint Security asigna a tales vulnerabilidades el estado *Oculto*.

La lista de vulnerabilidades aparece con forma de tabla. Cada fila de la tabla contiene la siguiente información:

- Un icono que representa el nivel de gravedad de la vulnerabilidad. Los niveles de criticidad de vulnerabilidades que existen son los siguientes:
 - Icono 🚨. **Crítico**. Este nivel de gravedad se aplica a las vulnerabilidades muy peligrosas que deben corregirse de inmediato. Los intrusos aprovechan de forma activa las vulnerabilidades de este nivel para infectar el sistema operativo del equipo o acceder a los datos personales del usuario. Kaspersky recomienda que se tomen lo antes posible todas las medidas necesarias para corregir las vulnerabilidades del nivel de gravedad "Crítico".
 - Icono ⚠️. **Importante**. Este nivel de gravedad se aplica a vulnerabilidades importantes que deben corregirse con la mayor brevedad posible. Los intrusos pueden aprovechar de forma activa las vulnerabilidades de este nivel. Actualmente, los intrusos no pueden aprovechar de forma activa las vulnerabilidades del nivel de gravedad "Importante". Kaspersky recomienda que se tomen lo antes posible todas las medidas necesarias para corregir las vulnerabilidades del nivel de gravedad "Importante".
 - Icono ⓘ. **Advertencia**. Este nivel de gravedad se aplica a las vulnerabilidades para las que puede posponerse la corrección. Sin embargo, dichas vulnerabilidades pueden amenazar la seguridad del equipo en el futuro.
- ID de vulnerabilidad.
- Nombre de la aplicación en la que se ha detectado la vulnerabilidad.
- Breve descripción de la vulnerabilidad.
- Información acerca del editor de software, tal como se indica en la firma digital.
- Resultado de las medidas tomadas para corregir la vulnerabilidad.

Nuevo inicio de la tarea Análisis de vulnerabilidades

Para actualizar la información sobre las vulnerabilidades detectadas previamente, puede reiniciar la tarea Análisis de vulnerabilidades. Es posible que deba reiniciar la tarea de análisis si el análisis de vulnerabilidades se interrumpió por algún motivo o si desea analizar el equipo en busca de vulnerabilidades después de la última [actualización de bases de datos y módulos de la aplicación](#).

Para iniciar de nuevo la tarea Análisis de vulnerabilidades:

1. Abra la [ventana principal de la aplicación](#).
2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Cuarentena** para abrir la ventana **Almacenes**.
3. En la ventana **Almacenes**, seleccione la pestaña **Vulnerabilidades**.
La pestaña **Vulnerabilidades** contiene una lista de las vulnerabilidades que ha detectado Kaspersky Endpoint Security durante la tarea Análisis de vulnerabilidades.
4. En la esquina inferior derecha de la ventana **Almacenes**, haga clic en el botón **Volver a analizar**.

En la lista de vulnerabilidades, Kaspersky Endpoint Security actualiza la información detallada relativa a las vulnerabilidades.

El estado de una vulnerabilidad que se ha corregido mediante la instalación de un parche propuesto no cambia tras otro análisis de vulnerabilidades.

Arreglo de vulnerabilidades

Puede corregir una vulnerabilidad mediante la instalación de una actualización del sistema operativo, el cambio de la configuración de una aplicación o la instalación de un parche de aplicaciones.

Es posible que las vulnerabilidades detectadas no se apliquen a las aplicaciones instaladas, sino a sus copias. Un parche puede corregir una vulnerabilidad solo si se instala la aplicación.

Para corregir una vulnerabilidad, haga lo siguiente:

1. Abra la [ventana principal de la aplicación](#).

2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Cuarentena** para abrir la ventana **Almacenes**.

3. En la ventana **Almacenes**, seleccione la pestaña **Vulnerabilidades**.

La pestaña **Vulnerabilidades** contiene una lista de las vulnerabilidades que ha detectado Kaspersky Endpoint Security durante la tarea Análisis de vulnerabilidades.

4. En la lista de vulnerabilidades, seleccione la entrada que corresponda a la vulnerabilidad pertinente.

En la parte inferior de la lista de vulnerabilidades, se abre una sección con información sobre la vulnerabilidad y las recomendaciones sobre cómo corregirla.

La siguiente información está disponible para cada una de las vulnerabilidades seleccionadas:

- Nombre de la aplicación en la que se ha detectado la vulnerabilidad.
- Versión de la aplicación en la que se ha detectado la vulnerabilidad.
- Nivel de gravedad de una vulnerabilidad.
- ID de vulnerabilidad.
- Fecha y hora de la última detección de vulnerabilidades.
- Recomendaciones sobre la corrección de vulnerabilidades (por ejemplo, un enlace a un sitio web con una actualización de sistema operativo o un parche de aplicaciones).
- Enlace a un sitio web con una descripción de la vulnerabilidad.

5. Para ver una descripción detallada de la vulnerabilidad, haga clic en el enlace **Información adicional** para abrir la página web que incluye una descripción de la amenaza que se ha asociado a la vulnerabilidad seleccionada. El sitio web www.secunia.com le permite descargar la actualización necesaria para la versión actual de la aplicación e instalarla.

6. Seleccione una de las siguientes formas para corregir una vulnerabilidad:

- Si hay uno o varios parches disponibles para la aplicación, instale el parche necesario siguiendo las instrucciones que se proporcionan junto al nombre del parche.
- Si hay una actualización del sistema operativo disponible, instale la actualización necesaria siguiendo las instrucciones que se proporcionan junto al nombre de la actualización.

La vulnerabilidad se corrige después de instalar el parche o la actualización. Kaspersky Endpoint Security asigna a esta vulnerabilidad un estado que significa que se ha corregido la vulnerabilidad. La entrada sobre la vulnerabilidad corregida aparece en gris en la lista de vulnerabilidades.

7. Si no se proporciona información sobre cómo arreglar una vulnerabilidad en la parte inferior de la ventana, puede ejecutar la tarea Análisis de vulnerabilidades de nuevo, tras la actualización de los módulos y las bases de datos de Kaspersky Endpoint Security. Puesto que Kaspersky Endpoint Security analiza el sistema en busca de vulnerabilidades (tomando como referencia una base de datos de vulnerabilidades), puede aparecer una entrada sobre una vulnerabilidad corregida tras la actualización de la aplicación.

Ocultación de entradas en la lista de vulnerabilidades

Puede ocultar una entrada de vulnerabilidad seleccionada. Kaspersky Endpoint Security asigna el estado *Oculto* a las entradas seleccionadas en la lista de vulnerabilidades y marcadas como ocultas. A continuación, puede [filtrar la lista de vulnerabilidades por el valor de estado *Oculto*](#).

Para ocultar una entrada en la lista de vulnerabilidades:

1. Abra la [ventana principal de la aplicación](#).
2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Cuarentena** para abrir la ventana **Almacenes**.
3. En la ventana **Almacenes**, seleccione la pestaña **Vulnerabilidades**.
La pestaña **Vulnerabilidades** contiene una lista de las vulnerabilidades que ha detectado Kaspersky Endpoint Security durante la tarea Análisis de vulnerabilidades.
4. En dicha lista de vulnerabilidades, seleccione la entrada de la vulnerabilidad que desea ocultar.
En la parte inferior de la lista de vulnerabilidades, se abre una sección con información sobre la vulnerabilidad y las recomendaciones sobre cómo corregirla.
5. Haga clic en el botón **Ocultar**.
Kaspersky Endpoint Security asigna el estado *Oculto* a la vulnerabilidad seleccionada. Las entradas de las vulnerabilidades con el estado *Oculto* se sitúan al final de la lista de vulnerabilidades y aparecen en gris.
6. Para ocultar una entrada sobre una vulnerabilidad en la lista de vulnerabilidades, seleccione la casilla de verificación **Oculto** en la parte superior de la lista.

Filtrado de la lista de vulnerabilidades por nivel de gravedad

Para filtrar la lista de vulnerabilidades por nivel de gravedad:

1. Abra la [ventana principal de la aplicación](#).

2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Cuarentena** para abrir la ventana **Almacenes**.

3. En la ventana **Almacenes**, seleccione la pestaña **Vulnerabilidades**.

La pestaña **Vulnerabilidades** contiene una lista de las vulnerabilidades que ha detectado Kaspersky Endpoint Security durante la tarea Análisis de vulnerabilidades. Aparecerán tres iconos según el nivel de gravedad de la vulnerabilidad (Advertencia, Importante, Crítico) en la parte superior de la lista de vulnerabilidades, en la fila **Mostrar gravedad**. Si hace clic en dichos iconos, podrás filtrar la lista de vulnerabilidades según el nivel de gravedad.

4. Haga clic en uno o varios de los iconos de nivel de gravedad de la vulnerabilidad. En la lista se mostrarán las vulnerabilidades que coincidan con los niveles de gravedad. Si no desea que se muestren en la lista las vulnerabilidades que coincidan con un nivel de gravedad específico, haga clic de nuevo en el icono de nivel de gravedad correspondiente. Si no se selecciona ningún nivel de gravedad, la lista de vulnerabilidades no mostrará nada.

Las condiciones especificadas de filtrado de entradas de vulnerabilidad se almacenan después de cerrar la ventana **Almacenes**.

Filtrado de la lista de vulnerabilidades por valores de estado Arreglado u Oculto

Para filtrar la lista de vulnerabilidades por valores de estado Arreglado u Oculto:

1. Abra la [ventana principal de la aplicación](#).

2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Cuarentena** para abrir la ventana **Almacenes**.

3. En la ventana **Almacenes**, seleccione la pestaña **Vulnerabilidades**.

La pestaña **Vulnerabilidades** contiene una lista de las vulnerabilidades que ha detectado Kaspersky Endpoint Security durante la tarea Análisis de vulnerabilidades.

4. Active las casillas de verificación que señalan el estado de las vulnerabilidades que se muestran junto al parámetro **Mostrar vulnerabilidades**. Para filtrar la lista de vulnerabilidades mediante el estado *Arreglado*, lleve a cabo una de las siguientes acciones:

- Para mostrar entradas sobre las vulnerabilidades arregladas en la lista de vulnerabilidades, seleccione la casilla de verificación **Arreglado**. Las entradas sobre vulnerabilidades arregladas tienen color gris en la lista de vulnerabilidades.
- Para ocultar entradas sobre las vulnerabilidades arregladas en la lista de vulnerabilidades, desactive la casilla de verificación **Arreglado**.

5. Para filtrar la lista de vulnerabilidades mediante el estado *Oculto*, lleve a cabo una de las siguientes acciones:

- Para mostrar entradas sobre las vulnerabilidades ocultas en la lista de vulnerabilidades, seleccione la casilla de verificación **Oculto**. Las entradas sobre vulnerabilidades ocultas tienen color gris en la lista de vulnerabilidades.
- Para ocultar entradas sobre las vulnerabilidades ocultas en la lista de vulnerabilidades, desactive la casilla de verificación **Oculto**.

Las condiciones especificadas de filtrado de entradas de vulnerabilidad no se almacenan después de cerrar la ventana **Almacenes**.

Comprobar la integridad de los módulos de la aplicación

Esta sección contiene información sobre los datos concretos y la configuración de la tarea de comprobación de integridad.

Acerca de la tarea Comprobación de integridad

Kaspersky Endpoint Security realiza una comprobación de los módulos de la aplicación en la carpeta de instalación de la aplicación en busca de datos corruptos o modificaciones. Si un módulo de la aplicación tiene una firma digital incorrecta, el módulo se considera corrupto.

Una vez que [se inicia la tarea Comprobación de integridad](#), se muestra su progreso en el campo situado junto al nombre de la tarea de la sección **Tareas**, en la pestaña **Protección y control** de la ventana principal de Kaspersky Endpoint Security.

Los resultados de la tarea de comprobación de integridad se registran en [informes](#).

Iniciar o detener una tarea de comprobación de integridad

Con independencia del modo de ejecución seleccionado, puede iniciar o detener una tarea de comprobación de integridad en cualquier momento.

Para iniciar o detener una tarea de comprobación de integridad:

1. Abra la [ventana principal de la aplicación](#).
2. Seleccione la pestaña **Protección y control**.
3. Abra la sección **Tareas**.
4. Haga clic con el botón derecho para que aparezca el menú contextual de la línea con el nombre de la tarea de comprobación de integridad.
5. Realice una de las siguientes acciones:
 - Para ejecutar la tarea Comprobación de integridad, seleccione **Iniciar análisis** en el menú.
El estado del progreso de la tarea que se muestra a la derecha del botón con el nombre de esta tarea cambia a *En ejecución*.
 - Si desea detener la tarea de comprobación de integridad, seleccione **Detener análisis** en el menú.
El estado del progreso de la tarea que se muestra a la derecha del botón con el nombre de esta tarea cambia a *Detenido*.

Seleccionar el modo de ejecución para la tarea de comprobación de la integridad

Para seleccionar el modo de ejecución de la tarea de comprobación de integridad:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Tareas planificadas**, seleccione **Comprobación de integridad**.
En la parte derecha de la ventana, se muestra la configuración de la tarea Comprobación de integridad.
3. En la sección **Modo de ejecución**, elija una de las opciones siguientes:
 - Si quiere iniciar una tarea Comprobación de integridad manualmente, seleccione **Manual**.
 - Si quiere configurar una planificación de inicio para la tarea de comprobación de integridad, seleccione **Mediante planificación**.
4. Si seleccionó la opción **Mediante planificación** durante el paso anterior, especifique la opción de planificación de la tarea. Para ello:
 - a. En la lista desplegable **Frecuencia**, especifique cuándo va a iniciarse la tarea de comprobación de integridad. Seleccione una de las siguientes opciones: **Minutos**, **Horas**, **Días**, **Cada semana**, **A la hora especificada**, **Cada mes** o **Después de iniciar la aplicación**.
 - b. Dependiendo del elemento seleccionado en la lista desplegable **Frecuencia**, especifique los valores de los parámetros que definen el momento del inicio de la tarea.
 - c. Si quiere que Kaspersky Endpoint Security ejecute tareas de Comprobación de integridad ignoradas lo antes posible, seleccione la casilla de verificación **Ejecutar tareas ignoradas**.


Si se selecciona **Después de iniciar la aplicación**, **Minutos** u **Horas** en la lista desplegable **Frecuencia**, la casilla de verificación **Ejecutar tareas ignoradas** ya no está disponible.
 - d. Si desea que Kaspersky Endpoint Security suspenda una tarea cuando los recursos informáticos sean limitados, seleccione la casilla de verificación **Ejecutar solo cuando el equipo está inactivo**.
Esta opción de planificación ayuda a ahorrar recursos del equipo.
5. Haga clic en **Aceptar**.
6. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Gestión de informes

Esta sección describe cómo configurar los parámetros de los informes y cómo gestionar los informes.

Principios de la gestión de informes

Información acerca del funcionamiento de cada componente de Kaspersky Endpoint Security, rendimiento de cada tarea de análisis, tarea de actualización, tarea de control de integridad y tarea de análisis de vulnerabilidades; además, el funcionamiento global de la aplicación se registra en informes.

Los datos del informe se presentan en forma de una tabla que contiene una lista de los eventos. Cada línea de la tabla contiene información sobre un evento independiente. Los atributos de eventos se encuentran en las columnas de la tabla. Algunas de las columnas son compuestas, que contienen columnas anidadas con atributos adicionales. Para ver atributos adicionales, debe pulsar el botón  situado junto al nombre del gráfico. Los eventos que se registran durante el funcionamiento de los diversos componentes o el rendimiento de las distintas tareas cuentan con distintos grupos de atributos.

Están disponibles los siguientes informes:

- Informe **Auditoría del sistema**. Contiene información acerca de los eventos producidos durante la interacción entre el usuario y la aplicación, y durante el funcionamiento de la aplicación en general, que no está relacionado con ningún componente o tarea de Kaspersky Endpoint Security en particular.
- Informe **Todos los componentes de protección**. Contiene información sobre los eventos que se han registrado durante el funcionamiento de los siguientes componentes de Kaspersky Endpoint Security:
 - Antivirus de archivos
 - Antivirus del correo.
 - Antivirus Internet.
 - Antivirus para chat.
 - System Watcher.
 - Firewall.
 - Prevención de intrusiones.
 - Prevención de ataques de BadUSB.
- Informe sobre el funcionamiento de un componente de o la ejecución de una tarea de Kaspersky Endpoint Security.
- Informe **Cifrado**. Contiene información sobre eventos que tienen lugar durante el cifrado y el descifrado de datos.

Los informes usan los siguientes niveles de importancia de eventos:

- **Eventos informativos**. Icono . Eventos formales que, por lo general, no contienen información importante.

- **Eventos importantes.** Icono 🚩. Eventos a los que se debe prestar atención porque reflejan situaciones importantes en el funcionamiento de Kaspersky Endpoint Security.
- **Eventos críticos.** Icono 🔴. Eventos de importancia fundamental que indican problemas en el funcionamiento de Kaspersky Endpoint Security o vulnerabilidades en la protección del equipo del usuario.

Para un procesamiento apropiado de los informes, puede modificar la presentación de los datos en la pantalla de los modos siguientes:

- Filtrado de la lista de eventos por diversos criterios.
- Uso de la función de búsqueda para buscar un determinado evento.
- Visualización del evento seleccionado en una sección independiente.
- Orden de las listas de eventos por cada columna del informe.
- Muestre y oculte eventos agrupados por el filtro de eventos.
- Cambio del orden y la disposición de las columnas que se muestran en el informe.

Puede guardar un informe generado en un archivo de texto, si es necesario.

También puede [eliminar información de informes](#) sobre las tareas y los componentes de Kaspersky Endpoint Security que se combinan en grupos. Kaspersky Endpoint Security elimina todas las entradas de los informes seleccionados desde la primera entrada hasta la hora actual.

Configuración de los parámetros de los informes

Puede configurar los parámetros de informes de las formas siguientes:

- Configure el período máximo de almacenamiento de los informes.
El período de almacenamiento máximo predeterminado de los informes sobre eventos registrados por Kaspersky Endpoint Security es de 30 días. Después de dicho período de tiempo, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo del informe. Puede cancelar la restricción basada en el tiempo o modificar la duración máxima de almacenamiento de informes.
- Configure el tamaño máximo del archivo del informe.
Puede especificar el tamaño máximo del archivo que contiene el informe. De forma predeterminada, el tamaño máximo de archivo del informe es de 1024 MB. Para evitar superar el tamaño máximo de archivo de informe, Kaspersky Endpoint Security elimina automáticamente las entradas más antiguas del archivo de informe cuando se alcance el tamaño máximo en el archivo de informe. Puede cancelar el límite de tamaño del archivo del informe o definir un valor diferente.

Configuración del período máximo de almacenamiento del informe

Para modificar el plazo máximo de almacenamiento de informes:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y almacenes**.

3. En la parte derecha de la ventana, en la sección **Parámetros del informe**, lleve a cabo una de las siguientes acciones:

- Para limitar el plazo de almacenamiento de los informes, seleccione la casilla de verificación **Conservar informes un máximo de**. En el campo situado junto a la casilla de verificación **Conservar informes un máximo de**, especifique el plazo máximo de almacenamiento de informes.

El período máximo predeterminado del almacenamiento de informes es de 30 días.

- Para cancelar el límite del plazo de almacenamiento de informes, desactive la selección del botón **Conservar informes un máximo de**.

El límite del plazo de almacenamiento de informes está activado de forma predeterminada.

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Configuración del tamaño máximo del archivo del informe

Para configurar el tamaño máximo del archivo del informe, haga lo siguiente:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y almacenes**.

3. En la parte derecha de la ventana, en la sección **Parámetros del informe**, realice una de las siguientes acciones:

- Para limitar el tamaño de archivo del informe, seleccione la casilla de verificación **Tamaño máximo de archivo**. En el campo situado a la derecha de la casilla de verificación **Tamaño máximo de archivo**, especifique el tamaño máximo del archivo de informe.

De forma predeterminada, el tamaño de archivo del informe está limitado a 1024 MB.

- Para quitar este límite del tamaño del archivo del informe, desactive la casilla de verificación **Tamaño máximo de archivo**.

El límite del tamaño de archivo del informe está activado de forma predeterminada.

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Visualización de informes

Para visualizar informes:

1. Abra la [ventana principal de la aplicación](#).

2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Informes** para abrir la ventana **Informes**.

3. Para generar el informe Todos los componentes de protección, en la parte izquierda de la ventana **Informes**, seleccione el elemento **Todos los componentes de protección** de la lista de componentes y tareas.

El informe Todos los componentes de protección se mostrará en la parte derecha de la ventana y contiene una lista de eventos del funcionamiento de todos los componentes de Kaspersky Endpoint Security.

4. Para generar un informe sobre el funcionamiento de un componente o tarea, en la lista de componentes y tareas a la izquierda de la ventana **Informes**, seleccione un componente o tarea.

En la parte derecha de la ventana, se muestra un informe que contiene una lista de eventos en el funcionamiento del componente o tarea seleccionado de Kaspersky Endpoint Security.

De forma predeterminada, los eventos del informe se clasifican por orden ascendente de los valores en la columna **Fecha del evento**.

Ver información de eventos en un informe

En el informe, podrás ver un resumen detallado de cada evento.

Para ver el resumen detallado de un evento en el informe:

1. Abra la [ventana principal de la aplicación](#).
2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Informes** para abrir la ventana **Informes**.
3. En la parte izquierda de la ventana, seleccione el informe correspondiente sobre el componente o tarea.
Los eventos que entran dentro del ámbito del informe se muestran en la tabla de la parte derecha de la ventana. Para encontrar eventos específicos en el informe, utilice las funciones de filtro, búsqueda y ordenación.
4. Seleccione el evento pertinente en el informe.

En la parte inferior de la ventana se muestra una sección con el resumen de eventos.

Almacenamiento de informes en archivos

Puede guardar el informe que se genera en un archivo en formato de texto (TXT) o un archivo CSV.

Kaspersky Endpoint Security registra eventos en el informe tal y como se muestran en la pantalla, es decir, con el mismo conjunto y secuencia de atributos de eventos.

Para guardar el informe en un archivo:

1. Abra la [ventana principal de la aplicación](#).
2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Informes** para abrir la ventana **Informes**.
3. Realice una de las siguientes acciones:
 - Para crear el informe "Todos los componentes de protección", seleccione **Todos los componentes de protección** en la lista de componentes y tareas.
El informe "Todos los componentes de protección" se mostrará en la parte derecha de la ventana y contiene una lista de eventos del funcionamiento de todos los componentes de protección.
 - Para generar un informe sobre el funcionamiento de un componente o tarea específicos, seleccione este componente o tarea en la lista de componentes y tareas.

En la parte derecha de la ventana se muestra un informe, que contiene una lista de eventos en el funcionamiento del componente o la tarea seleccionados.

4. Si fuera necesario, puede modificar la presentación de los datos en el informe haciendo lo siguiente:

- Filtrando eventos
- Realizando una búsqueda de eventos
- Reorganizando columnas
- Ordenando eventos

5. Haga clic en el botón **Guardar informe** en la parte superior derecha de la ventana.

Se abre un menú contextual.

6. En el menú contextual, seleccione la codificación para guardar el archivo del informe: **Guardar como ANSI** o **Guardar como Unicode**.

Se abre la ventana estándar **Guardar como** de Microsoft Office.

7. En la ventana **Guardar como**, especifique la carpeta de destino para el archivo del informe.

8. En el campo **Nombre del archivo**, escriba el nombre del archivo del informe.

9. En el campo **Tipo de archivo**, seleccione el formato del archivo del informe necesario: TXT o CSV.

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

Limpieza de informes

Para quitar información de los informes:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y almacenes**.

3. En la parte derecha de la ventana, en la sección **Parámetros del informe**, haga clic en el botón **Eliminar informes**.

Se abre la ventana **Limpiar informes**.

4. Seleccione las casillas de verificación de los informes de los que quiera eliminar información:

- **Todos los informes.**
- **Informe general de protección.** Contiene información sobre el funcionamiento de los siguientes componentes de Kaspersky Endpoint Security:
 - Antivirus de archivos
 - Antivirus del correo.
 - Antivirus Internet.

- Antivirus para chat.
- System Watcher.
- Firewall.
- Prevención de intrusiones.
- Prevención de ataques de BadUSB.
- **Informe de tareas de análisis.** Contiene información sobre tareas de análisis completadas:
 - Análisis completo
 - Análisis de áreas críticas
 - Análisis personalizado
 - Comprobación de integridad.
- **Informe de tareas de actualización.** Contiene información sobre las tareas de actualización completadas:
- **Informe de Firewall.** Contiene información sobre el funcionamiento de Firewall.
- **Informe de componentes de control.** Contiene información sobre el funcionamiento de los siguientes componentes de Kaspersky Endpoint Security:
 - Control de inicio de aplicaciones.
 - Control de actividad de aplicaciones.
 - Control de vulnerabilidades.
 - Control de dispositivos.
 - Control web.
- **Informe de cifrado de datos.**

5. Haga clic en **Aceptar**.

Servicio de notificaciones

Esta sección contiene información sobre el servicio de notificaciones que alerta al usuario acerca de eventos en el funcionamiento de Kaspersky Endpoint Security. También contiene instrucciones sobre los parámetros de notificaciones.

Acerca de las notificaciones de Kaspersky Endpoint Security

Toda clase de eventos se producen durante el funcionamiento de Kaspersky Endpoint Security. Pueden ser puramente informativos o críticos. Por ejemplo, las notificaciones pueden informar de una actualización de base de datos y de módulo de aplicación exitosa o registrar errores de componentes que se necesitan remediar.

Kaspersky Endpoint Security admite el registro de información sobre eventos en el funcionamiento del registro de aplicaciones de Microsoft Windows y / o del registro de sucesos de Kaspersky Endpoint Security.

Kaspersky Endpoint Security envía notificaciones de las siguientes formas:

- mediante notificaciones emergentes en el área de notificación de la barra de tareas de Microsoft Windows;
- por correo electrónico.

Puede configurar el envío de notificaciones de eventos. El método de envío de notificaciones se configura para cada tipo de evento.

Configuración del servicio de notificaciones

Puede llevar a cabo las siguientes acciones para configurar el servicio de notificaciones:

- Configure la configuración de los registros de eventos donde Kaspersky Endpoint Security registre eventos.
- Configure la manera en que se muestran las notificaciones en pantalla.
- Configure el envío de notificaciones por correo electrónico.

Al usar la tabla de eventos para configurar el servicio de notificaciones, puede realizar las siguientes acciones:

- Filtre los eventos del servicio de notificaciones por valores de columnas o por condiciones de filtro personalizadas.
- Utilice la función de búsqueda para los eventos del servicio de notificaciones.
- Ordene los eventos del servicio de notificaciones.
- Cambie el orden y el conjunto de columnas que aparecen en la lista de eventos del servicio de notificaciones.

Configuración de los parámetros de registro de eventos

Para configurar los parámetros del registro de eventos:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y almacenes**.
La parte derecha de la ventana muestra la configuración de los informes y el almacenamiento.
3. En la sección **Notificaciones**, haga clic en el botón **Configuración**.
Esto abre la ventana **Notificaciones**.
Los componentes y tareas de Kaspersky Endpoint Security aparecen en la parte izquierda de la ventana. En la parte derecha de la ventana figuran los eventos generados del componente o tarea seleccionados.
4. En la parte izquierda de la ventana, seleccione el componente o la tarea para los que desee configurar los parámetros del registro de eventos.
5. Seleccione las casillas de verificación de los eventos relevantes de las columnas **Guardar en registro local** y **Guardar en Registro de eventos de Windows**.
Los eventos cuyas casillas de verificación están seleccionadas en la columna **Guardar en registro local** se muestran en **Registros de aplicaciones y servicios** en la sección **Registro de eventos de Kaspersky**. Los eventos cuyas casillas de verificación están seleccionadas en la columna **Guardar en Registro de eventos de Windows** se muestran en **Registros de Windows** en la sección **Aplicación**. Para abrir los registros de eventos, haga clic en **Ejecutar** → **Panel de control** → **Administración** → **Visor de eventos**.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Configuración de la visualización y entrega de notificaciones

Para configurar la visualización y entrega de notificaciones:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y almacenes**.
La parte derecha de la ventana muestra la configuración de los informes y el almacenamiento.
3. En la sección **Notificaciones**, haga clic en el botón **Configuración**.
Esto abre la ventana **Notificaciones**.
Los componentes y tareas de Kaspersky Endpoint Security aparecen en la parte izquierda de la ventana. En la parte derecha de la ventana, figuran los eventos generados del componente o la tarea seleccionados.
4. En la parte izquierda de la ventana, seleccione el componente o la tarea para los que desee configurar el envío de notificaciones.
5. En la columna **Notificar en pantalla**, seleccione las casillas de verificación situadas junto a los eventos requeridos.
La información sobre los eventos seleccionados aparece en mensajes emergentes en pantalla en el área de notificación de la barra de tareas de Microsoft Windows.
6. En la columna **Notificar por correo electrónico**, seleccione las casillas de verificación situadas junto a los eventos requeridos.
La información sobre los eventos seleccionados se entrega por correo electrónico si se configuran los ajustes de entrega de notificaciones del correo.

7. Haga clic en el botón **Parámetros de notificaciones por correo**.

Esto abre la ventana **Parámetros de notificaciones por correo**.

8. Seleccione la casilla de verificación **Enviar notificaciones de eventos** para activar el envío de notificaciones sobre los eventos de Kaspersky Endpoint Security que se seleccionan en la columna **Notificar por correo electrónico**.

9. Especifique la configuración del envío de notificaciones por correo electrónico.

10. Haga clic en **Aceptar**.

11. En la ventana **Parámetros de notificaciones por correo**, haga clic en **Aceptar**.

12. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Configuración de la visualización de advertencias sobre el estado de la aplicación en el área de notificaciones

Para configurar la visualización de advertencias de estado de la aplicación en el área de notificaciones:



1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Interfaz**.

La configuración de la interfaz de Kaspersky Endpoint Security se muestra en la parte derecha de la ventana.

3. En la sección **Advertencias**, seleccione las casillas de verificación que hay junto a esas categorías de eventos sobre los cuales desea ver notificaciones en el área de notificaciones de Microsoft Windows.

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Cuando tienen lugar eventos asociados con las categorías seleccionadas, el [icono de la aplicación](#) del área de notificaciones cambiará a  o a  según la seriedad de la advertencia.

Gestión de Cuarentena y Respaldo

Esta sección describe el modo de configurar y gestionar Cuarentena y Respaldo.

Acerca de Cuarentena y Respaldo

Cuarentena es una lista de archivos probablemente infectados. Los *archivos probablemente infectados* son aquellos que pueden contener virus y otras amenazas, o bien una variedad de estos.

Cuando Kaspersky Endpoint Security pone en cuarentena un archivo probablemente infectado, no copia el archivo, sino que lo mueve: la aplicación elimina el archivo del disco duro o del mensaje de correo electrónico y guarda el archivo en un almacén de datos especial. Los archivos en Cuarentena se guardan en un formato especial y no suponen amenaza alguna.

Kaspersky Endpoint Security puede detectar y poner en cuarentena un archivo probablemente infectado mientras se ejecuta un [análisis antivirus](#) y también durante el funcionamiento de los componentes [Antivirus de archivos](#), [Antivirus del correo](#) y [System Watcher](#).

Kaspersky Endpoint Security pone archivos en cuarentena en los casos siguientes:

- El código del archivo recuerda a un programa malicioso conocido aunque parcialmente modificado, o tiene una estructura similar a la del software malicioso (malware), y no aparece en la base de datos de Kaspersky Endpoint Security. En este caso, el archivo se pone en cuarentena después del análisis heurístico realizado mediante Antivirus de archivos y Antivirus del correo o durante un análisis antivirus. Los análisis heurísticos raramente provocan falsos positivos.
- La secuencia de operaciones que realiza un archivo es peligrosa. En este caso, el archivo se coloca en Cuarentena después de que el componente System Watcher haya analizado su comportamiento.

Respaldo es una lista de copias de respaldo de los archivos que se han eliminado o modificado durante el proceso de desinfección. La *copia de respaldo* es una copia del archivo creada cuando se intenta desinfectar o eliminar este archivo por primera vez. Las copias de respaldo de los archivos se almacenan en un formato especial y no suponen amenaza ninguna.

En ocasiones no se puede mantener la integridad de los archivos durante la desinfección. Si, después de la desinfección, pierde parcial o completamente el acceso a información importante de un archivo desinfectado, puede intentar restaurar la copia desinfectada de dicho archivo en su carpeta original.

Es posible que, después de otra actualización del módulo del software de la aplicación o la base de datos, Kaspersky Endpoint Security pueda identificar definitivamente la amenazas y neutralizarlas. Por lo tanto, se recomienda analizar los archivos de la cuarentena cada vez que se actualice el módulo del software de la aplicación y la base de datos.

Configuración de los parámetros de Cuarentena y Respaldo

El almacenamiento de datos consta de Cuarentena y Respaldo. Puede configurar los parámetros de Cuarentena y Respaldo del siguiente modo:

- Configure el plazo de almacenamiento máximo de archivos en Cuarentena y de las copias de archivos en Respaldo.

El plazo máximo de almacenamiento predeterminado de los archivos en Cuarentena y de las copias de los archivos en Respaldo es de 30 días. Cuando finaliza el plazo de almacenamiento máximo, Kaspersky Endpoint Security elimina los archivos más antiguos del almacén de datos. Puede cancelar la restricción basada en el tiempo o modificar la duración máxima de almacenamiento de objetos.

- Puede configurar el tamaño máximo de Cuarentena y Respaldo.

De forma predeterminada, el tamaño máximo de Cuarentena y Respaldo es de 100 MB. Cuando se alcanza el límite del almacenamiento de datos, Kaspersky Endpoint Security elimina automáticamente los archivos antiguos de Cuarentena y Respaldo para que no se supere el tamaño máximo de almacenamiento de datos. Puede cancelar el límite de tamaño de Cuarentena y Respaldo o cambiar su tamaño máximo.

Configuración del período de almacenamiento máximo de archivos en Cuarentena y de las copias de archivos en Respaldo

Para configurar el período de almacenamiento máximo de archivos en Cuarentena y de las copias de archivos en Respaldo, haga lo siguiente:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y almacenes**.
3. Realice una de las siguientes acciones:
 - Para limitar el período de almacenamiento de archivos de Cuarentena y Respaldo, en la sección **Configuración de Cuarentena y Respaldo** de la parte derecha de la ventana, seleccione la casilla de verificación **Conservar objetos un máximo de**. En el campo situado a la derecha de la casilla de verificación **Conservar objetos un máximo de**, especifique el período de almacenamiento máximo para los archivos en Cuarentena y las copias de los archivos en Respaldo. El período de almacenamiento para los archivos en Cuarentena y las copias de archivos de Respaldo está limitado a 30 días de forma predeterminada.
 - Para cancelar el límite del período de almacenamiento de archivos de Cuarentena y Respaldo, en la sección **Configuración de Cuarentena y Respaldo** de la parte derecha de la ventana, seleccione la casilla de verificación **Conservar objetos un máximo de**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Configuración del tamaño máximo de Cuarentena y Respaldo

Para configurar el tamaño máximo de Cuarentena y Respaldo, haga lo siguiente:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y almacenes**.
3. Realice una de las siguientes acciones:
 - Si desea limitar el tamaño total de Cuarentena y Copia de seguridad, seleccione la casilla de verificación **Tamaño máximo de almacenamiento** en la parte derecha de la ventana en la sección **Configuración de**

Cuarentena y Respaldo, y especifique el tamaño máximo de Cuarentena y Respaldo en el campo situado a la derecha de la casilla **Tamaño máximo de almacenamiento**.

De forma predeterminada, el tamaño máximo de almacenamiento para datos que comprenden el directorio Cuarentena y las copias de respaldo de los archivos es de 100 MB.

- Si desea eliminar el límite de tamaño de Cuarentena y Respaldo, desactive la casilla de verificación **Tamaño máximo de almacenamiento** situada en la parte derecha de la ventana en la sección **Configuración de Cuarentena y Respaldo**.

El tamaño de Cuarentena y Respaldo es ilimitado de forma predeterminada.

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Gestión de Cuarentena

Kaspersky Endpoint Security elimina automáticamente de cuarentena los [archivos eliminados](#) (independientemente de su estado), una vez que ha vencido el período de almacenamiento establecido en la configuración de la aplicación.

Las siguientes operaciones con archivos están disponibles al gestionar la Cuarentena:

- Ver los archivos puestos en cuarentena por Kaspersky Endpoint Security.
- Analizar archivos que pueden estar infectados con la versión actual de las bases de datos y los módulos de Kaspersky Endpoint Security.
- Restaurar los archivos de Cuarentena a sus carpetas originales.
- Quitar archivos de Cuarentena.
- Abra la carpeta en la que se encontraban originalmente los archivos.

El conjunto de los archivos en cuarentena se presenta como una tabla.

También puede llevar a cabo las siguientes acciones mientras gestiona los datos de la tabla:

- Filtrar archivos en cuarentena según las columnas y condiciones del filtro personalizado.
- Utilizar la función de búsqueda de archivos en cuarentena.
- Ordenar archivos en cuarentena.
- Cambiar el orden y el conjunto de columnas que se muestran en la lista de archivos en cuarentena.

Puede copiar los eventos en cuarentena seleccionados en el portapapeles. Para seleccionar varios archivos en cuarentena, haga clic con el botón derecho del ratón para abrir el menú contextual de cualquier archivo y elegir **Seleccionar todo**. Para anular la selección de archivos que no desea analizar, haga clic en ellos mientras mantiene pulsada la tecla **CTRL**.

Activación y desactivación del análisis de archivos en Cuarentena tras una actualización

Si Kaspersky Endpoint Security detecta signos de infección al analizar un archivo, pero no logra determinar qué programas maliciosos lo han infectado, Kaspersky Endpoint Security mueve este archivo a [Cuarentena](#). Kaspersky Endpoint Security puede identificar definitivamente las amenazas y neutralizarlas después de haber actualizado las bases de datos y los módulos de la aplicación. Puede activar el análisis automático de archivos en Cuarentena después de cada actualización de las bases de datos y los módulos de la aplicación.

Recomendamos analizar con regularidad los archivos de Cuarentena. Al analizar, puede cambiar el estado de los archivos. Algunos archivos pueden desinfectarse y restablecerse a sus ubicaciones originales, de modo que pueda seguir usándolos.

Para activar el análisis de archivos en cuarentena tras las actualizaciones:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione **Informes y almacenes**.
En la parte derecha de la ventana, se muestra la configuración de gestión para informes y almacenes.
3. En la sección **Configuración de Cuarentena y Respaldo**, realice una de las siguientes acciones:
 - Para activar el análisis de archivos en cuarentena después de cada actualización de Kaspersky Endpoint Security, seleccione la casilla de verificación **Volver a analizar la Cuarentena después de actualizar**.
 - Para desactivar el análisis de archivos en cuarentena después de cada actualización de Kaspersky Endpoint Security, desactive la casilla de verificación **Volver a analizar la Cuarentena después de actualizar**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Inicio de una tarea de análisis personalizado para archivos en Cuarentena

Después de la actualización de las bases de datos y de los módulos del software de la aplicación, Kaspersky Endpoint Security puede identificar las amenazas que existen en los archivos en cuarentena y neutralizarlos de forma definitiva. Si no se ha configurado la aplicación para analizar automáticamente archivos en cuarentena después de cada actualización de las bases de datos y los módulos de aplicaciones, puede iniciar manualmente una tarea de Análisis personalizado para archivos en cuarentena.

Para iniciar una tarea de Análisis personalizado para archivos en cuarentena, haga lo siguiente:

1. Abra la [ventana principal de la aplicación](#).
2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Cuarentena** para abrir la ventana **Almacenes**.
Se abre la pestaña **Cuarentena** de la ventana **Almacenes**.
3. En la pestaña **Cuarentena**, seleccione uno o varios archivos probablemente infectados que desee analizar.
Para seleccionar varios archivos en cuarentena, haga clic con el botón derecho del ratón para abrir el menú contextual de cualquier archivo y elegir **Seleccionar todo**. Para anular la selección de archivos que no desea analizar, haga clic en ellos mientras mantiene pulsada la tecla **CTRL**.

4. Inicie la tarea Análisis personalizado de una de las siguientes formas:

- Haga clic en el botón **Volver a analizar**.
- Haga clic con el botón derecho para que aparezca el menú contextual y seleccione **Volver a analizar**.

Cuando se ha completado el análisis, aparece una notificación con el número de archivos analizados y el número de amenazas detectadas.

Restauración de archivos de la Cuarentena

Para restaurar los archivos de Cuarentena, haga lo siguiente:

1. Abra la [ventana principal de la aplicación](#).

2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Cuarentena** para abrir la ventana **Almacenes**.

Se abre la pestaña **Cuarentena** de la ventana **Almacenes**.

3. Si desea restaurar todos los archivos en cuarentena, seleccione **Restaurar todos** desde el menú contextual de cualquier archivo.

Kaspersky Endpoint Security restaura todos los archivos de Cuarentena a sus carpetas originales.

4. Para restaurar uno o varios archivos en cuarentena, haga lo siguiente:

a. En la pestaña **Cuarentena**, seleccione uno o varios archivos que desee restaurar de Cuarentena.

Para seleccionar varios archivos en cuarentena, haga clic con el botón derecho del ratón para abrir el menú contextual de cualquier archivo y elegir **Seleccionar todo**. Para anular la selección de archivos que no desea analizar, haga clic en ellos mientras mantiene pulsada la tecla **CTRL**.

b. Restaure los archivos de uno de los siguientes modos:

- Haga clic en el botón **Restaurar**.
- Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Restaurar**.

Kaspersky Endpoint Security restaura los archivos seleccionados en sus carpetas originales.

Eliminación de archivos de la Cuarentena

Para eliminar los archivos de Cuarentena, haga lo siguiente:

1. Abra la [ventana principal de la aplicación](#).

2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Cuarentena** para abrir la ventana **Almacenes**.

Se abre la pestaña **Cuarentena** de la ventana **Almacenes**.

3. Si desea eliminar todos los archivos de la Cuarentena, seleccione **Eliminar todos** desde el menú contextual de cualquier archivo.

Kaspersky Endpoint Security elimina todos los archivos de Cuarentena.

4. Para eliminar uno o varios archivos en cuarentena, haga lo siguiente:

a. En la tabla de la pestaña **Cuarentena**, seleccione uno o varios archivos probablemente infectados que desee eliminar de Cuarentena.

Para seleccionar varios archivos en cuarentena, haga clic con el botón derecho del ratón para abrir el menú contextual de cualquier archivo y elegir **Seleccionar todo**. Para anular la selección de archivos que no desea analizar, haga clic en ellos mientras mantiene pulsada la tecla **CTRL**.

b. Elimine archivos de uno de los siguientes modos:

- Haga clic en el botón **Eliminar**.
- Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Eliminar**.

Kaspersky Endpoint Security elimina los archivos seleccionados de Cuarentena.

Gestión de Respaldo

Si se detecta código malicioso en el archivo, Kaspersky Endpoint Security lo bloquea, coloca una copia en Respaldo e intenta desinfectarlo. Si se realiza la desinfección del archivo correctamente, el estado de la copia de respaldo del archivo pasará a *Desinfectado*. El archivo está disponible en su carpeta original. Si un archivo no se puede desinfectar, Kaspersky Endpoint Security lo elimina de su carpeta original. Puede restaurar el archivo de su copia de seguridad a su carpeta original.

Al detectar código malicioso en un archivo que forma parte de la aplicación Tienda Windows, Kaspersky Endpoint Security elimina de inmediato el archivo sin que se mueva una copia del archivo a Respaldo. Puede restaurar la integridad de la aplicación de la Tienda Windows por medio de las herramientas adecuadas del sistema operativo Microsoft Windows 8 (consulte los *archivos de ayuda de Microsoft Windows 8* para obtener información detallada sobre la restauración de una aplicación de la Tienda Windows).

Kaspersky Endpoint Security [elimina automáticamente las copias de seguridad](#) de los archivos de Respaldo (independientemente de su estado), una vez que ha vencido el período de almacenamiento definido en la configuración de la aplicación.

También puede eliminar manualmente cualquier copia de un archivo desde Respaldo.

El conjunto de las copias de seguridad de los archivos se presenta como una tabla.

Al gestionar Respaldo, puede llevar a cabo las siguientes acciones con copias de respaldo de los archivos:

- Ver la lista de copias de seguridad de los archivos.
- Restaure los archivos de las copias de respaldo a sus carpetas originales.
- Elimine las copias de respaldo de los archivos de Respaldo.

También puede llevar a cabo las siguientes acciones mientras gestiona los datos de la tabla:

- Filtrar copias de seguridad por columnas, incluidas las condiciones de filtro personalizado.
- Utilizar la función de búsqueda de copias de seguridad.

- Ordenar copias de seguridad.
- Cambiar el orden y el conjunto de columnas que se muestran en la lista de copias de seguridad.

Puede copiar los eventos de Respaldo seleccionados en el portapapeles. Para seleccionar varios archivos de Respaldo, haga clic con el botón derecho del ratón para abrir el menú contextual de cualquier archivo y elija **Seleccionar todos**. Para anular la selección de archivos que no desea analizar, haga clic en ellos mientras mantiene pulsada la tecla **CTRL**.

Restauración de archivos de Respaldo

Para restaurar los archivos de Respaldo, haga lo siguiente:

1. Abra la [ventana principal de la aplicación](#).
2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Cuarentena** para abrir la ventana **Almacenes**.
3. En la ventana **Almacenes**, seleccione la pestaña **Respaldo**.
4. Si desea restaurar todos los archivos de Respaldo, seleccione **Restaurar todos** desde el menú contextual de cualquier archivo.

Kaspersky Endpoint Security restaura todos los archivos a partir de las copias de respaldo en las carpetas originales.

5. Para restaurar uno o varios archivos de Respaldo, haga lo siguiente:
 - a. En la tabla de la pestaña **Respaldo**, seleccione uno o varios archivos de Respaldo.
Para seleccionar varios archivos en cuarentena, haga clic con el botón derecho del ratón para abrir el menú contextual de cualquier archivo y elegir **Seleccionar todo**. Para anular la selección de archivos que no desea analizar, haga clic en ellos mientras mantiene pulsada la tecla **CTRL**.
 - b. Restaura los archivos de uno de los siguientes modos:
 - Haga clic en el botón **Restaurar**.
 - Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Restaurar**.

Kaspersky Endpoint Security restaura los archivos a partir de las copias de respaldo seleccionadas en las carpetas originales.

Eliminación de las copias de seguridad de los archivos de Respaldo

Para eliminar las copias de respaldo de los archivos de Respaldo:

1. Abra la [ventana principal de la aplicación](#).
2. En la parte superior de la ventana principal de la aplicación, haga clic en el enlace **Cuarentena** para abrir la ventana **Almacenes**.

3. En la ventana **Almacenes**, seleccione la pestaña **Respaldo**.

4. Si desea eliminar todos los archivos desde Respaldo, realice una de las acciones siguientes:

- En el menú contextual de cualquier archivo, seleccione **Eliminar todos**.
- Haga clic en el botón **Borrar almacén**.

Kaspersky Endpoint Security elimina todas las copias de respaldo de archivos desde Respaldo.

5. Si desea eliminar uno o varios archivos desde Respaldo:

a. En la tabla de la pestaña **Respaldo**, seleccione uno o varios archivos de Respaldo.

Para seleccionar varios archivos de Respaldo, haga clic con el botón derecho del ratón para abrir el menú contextual de cualquier archivo y elija **Seleccionar todos**. Para anular la selección de archivos que no desea analizar, haga clic en ellos mientras mantiene pulsada la tecla **CTRL**.

b. Elimine archivos de uno de los siguientes modos:

- Haga clic en el botón **Eliminar**.
- Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Eliminar**.

Kaspersky Endpoint Security elimina las copias de respaldo seleccionadas de los archivos de Respaldo.

Configuración avanzada de la aplicación

Esta sección describe la configuración avanzada de Kaspersky Endpoint Security y su configuración.

Crear y utilizar un archivo de configuración

Un archivo de configuración con los ajustes de Kaspersky Endpoint Security le permite llevar a cabo las tareas siguientes:

- Realice la instalación local de Kaspersky Endpoint Security mediante la línea de comandos con la configuración predefinida.
Para ello, debe guardar el archivo de configuración en la misma carpeta donde se ubica el kit de distribución.
- Realice la instalación remota de Kaspersky Endpoint Security mediante Kaspersky Security Center con la configuración predefinida.
- Migre la configuración de Kaspersky Endpoint Security de un equipo al otro.

Para crear un archivo de configuración:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Administrar parámetros**, haga clic en el botón **Guardar**.
Esto abre la ventana **Seleccione un archivo de configuración** estándar de Microsoft Windows.
4. Especifique la ruta en la cual desea guardar el archivo de configuración e introduzca su nombre.

Si desea usar el archivo de configuración para la instalación local o remota de Kaspersky Endpoint Security, lo debe denominar install.cfg.

5. Haga clic en el botón **Guardar**.

Para importar la configuración de Kaspersky Endpoint Security desde un archivo de configuración:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Administrar parámetros**, haga clic en el botón **Cargar**.
Esto abre la ventana **Seleccione un archivo de configuración** estándar de Microsoft Windows.
4. Especifique la ruta al archivo de configuración.
5. Haga clic en el botón **Abrir**.

Todos los valores de la configuración de Kaspersky Endpoint Security se definirán según el archivo de configuración seleccionado.

Zona de confianza

Esta sección contiene información sobre la zona de confianza y las instrucciones de configuración de exclusiones del análisis y creación de una lista de aplicaciones de confianza.

Acerca de la zona de confianza

Una *zona de confianza* es una lista de objetos y aplicaciones configurada por el administrador del sistema que Kaspersky Endpoint Security no supervisa cuando está activo. Dicho de otro modo: es un conjunto de exclusiones del análisis.

El administrador crea la zona de confianza de manera independiente y tiene en cuenta las características de los objetos que se gestionan y de las aplicaciones que se instalan en el equipo. Puede que sea necesario incluir objetos y aplicaciones en la zona de confianza cuando Kaspersky Endpoint Security bloquea el acceso a ellos, si está seguro de que el objeto o la aplicación son inofensivos.

Puede excluir los siguientes objetos del análisis:

- Archivos de ciertos formatos
- Archivos que una máscara ha seleccionado
- Archivos seleccionados
- Carpetas
- Procesos de aplicaciones

Exclusiones del análisis

Una *exclusión del análisis* es un conjunto de condiciones según las cuales Kaspersky Endpoint Security no analiza un objeto en busca de virus u otras amenazas.

Las exclusiones del análisis permiten utilizar de manera segura software legítimo que los delincuentes pueden utilizar para dañar el equipo o los datos del usuario. Aunque no poseen ninguna función maliciosa, dichas aplicaciones pueden emplearse como un componente auxiliar en el software malicioso (malware). Algunos ejemplos de dichas aplicaciones son: herramientas de administración remota, clientes IRC, servidores FTP, varias utilidades para suspender u ocultar procesos, registradores de teclado, copiadore de contraseñas y marcadores automáticos. Dichas aplicaciones no se clasifican como virus. Puede encontrar información acerca del software legal que pueden usar los delincuentes para dañar su equipo o sus datos personales en la enciclopedia del virus de Kaspersky en <https://encyclopedia.kaspersky.es/knowledge/riskware/>.

Es posible que Kaspersky Endpoint Security bloquee estas aplicaciones. Para evitar que se bloqueen, puede configurar las exclusiones del análisis para las aplicaciones en uso. Para ello, agregue el nombre o la máscara de nombre que figura en la Enciclopedia del virus de Kaspersky a la zona de confianza. Por ejemplo, es posible que utilice con frecuencia un programa Remote Administrator. Se trata de una aplicación de acceso remoto que le ofrece controlar un equipo de manera remota. Kaspersky Endpoint Security identifica esta actividad como sospechosa y puede que la bloquee. Para evitar el bloqueo de la aplicación, cree una exclusión del análisis con el nombre o la máscara de nombre que se muestra en la Enciclopedia del virus de Kaspersky.

Si la aplicación que recopila la información y la envía para procesarse se instala en su equipo, Kaspersky Endpoint Security puede clasificar esta aplicación como malware. Para evitar esto, puede excluir la aplicación del análisis al configurar Kaspersky Endpoint Security como se describe en este documento.

Los siguientes componentes de aplicaciones y tareas que el administrador del sistema configure pueden utilizar exclusiones del análisis:

- Antivirus de archivos
- Antivirus del correo.
- Antivirus Internet.
- Control de actividad de aplicaciones.
- Tareas de análisis
- System Watcher.

Lista de aplicaciones de confianza

La *lista de aplicaciones de confianza* es una lista de aplicaciones cuya actividad de red y archivos (incluida la actividad maliciosa), así como el acceso al registro del sistema, no supervisa Kaspersky Endpoint Security. De forma predeterminada, Kaspersky Endpoint Security analiza los objetos que el proceso de cualquier programa abre, ejecuta o guarda, y controla la actividad de todas las aplicaciones y el tráfico de red que generan. Kaspersky Endpoint Security excluye del análisis las aplicaciones de la [lista de aplicaciones de confianza](#).

Por ejemplo, si considera que los objetos que emplea el Bloc de notas estándar de Microsoft Windows son seguros sin necesidad de analizarlos, significa que confía en esta aplicación y que puede agregar el Bloc de notas de Microsoft Windows a la lista de aplicaciones de confianza. Por tanto, el análisis no incluirá objetos que emplee esta aplicación.

Además, algunas acciones que Kaspersky Endpoint Security clasifica como sospechosas pueden ser seguras dentro del contexto de la funcionalidad de diferentes aplicaciones. Por ejemplo, la interceptación de texto que se escribe mediante el teclado es un proceso rutinario para intercambiadores de disposición del teclado automáticos (como Punto Switcher). Para tener en cuenta los detalles de este tipo de aplicaciones y excluir su actividad del proceso de análisis, le recomendamos que las agregue a la lista de aplicaciones de confianza.

La exclusión de aplicaciones de confianza del proceso de análisis permite evitar conflictos de compatibilidad entre Kaspersky Endpoint Security y otros programas (por ejemplo, el problema de analizar dos veces el tráfico de red de un equipo de terceros, por parte de Kaspersky Endpoint Security y de otra aplicación antivirus) y también aumenta el rendimiento del equipo, que es fundamental cuando se emplean aplicaciones de servidor.

Al mismo tiempo, el archivo ejecutable y el proceso de la aplicación de confianza sí que se analizan en busca de virus y otro software malicioso (malware). Puede excluirse completamente una aplicación del análisis de Kaspersky Endpoint Security gracias a las exclusiones del análisis.

Creación de una exclusión del análisis

Kaspersky Endpoint Security no analiza un objeto si la unidad de disco o la carpeta que contiene este objeto se incluyen en la cobertura del análisis al inicio de una de las tareas de análisis. Sin embargo, no se aplica la exclusión del análisis cuando se inicia una tarea de análisis personalizado para este objeto en particular.

Para crear una exclusión del análisis:

1. Abra la [ventana de configuración de la aplicación](#).

2. Seleccione la sección **Protección Antivirus** situada a la izquierda.

La configuración de la protección antivirus se muestra en la parte derecha de la ventana.

3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.

Se abre la ventana **Zona de confianza** en la pestaña **Exclusiones del análisis**.

4. Haga clic en el botón **Agregar**.

Se abre la ventana **Exclusión del análisis**. En esta ventana, puede crear una exclusión de análisis con el o los criterios de la sección **Propiedades**.

5. Para excluir un archivo o una carpeta del análisis:

a. En la sección **Propiedades**, seleccione la casilla de verificación **Archivo o carpeta**.

b. Haga clic en el enlace **Seleccionar archivo o carpeta** de la sección **Descripción de la exclusión del análisis** para abrir la ventana **Nombre de archivo o carpeta**.

c. Introduzca el archivo o el nombre de la carpeta, o bien la máscara del archivo o del nombre de carpeta. También puede seleccionar el archivo o carpeta en el árbol de carpetas haciendo clic en **Examinar**.

La máscara del nombre de archivo o carpeta puede contener el asterisco (*) en reemplazo de cualquier número de caracteres del nombre de archivo.

Por ejemplo, puede usar máscaras para agregar las siguientes rutas:

- Rutas a los archivos de cualquier carpeta:
 - La máscara "*.exe" comprende las rutas a todos los archivos de extensión EXE.
 - La máscara "prueba" comprende las rutas a todos los archivos de nombre "prueba".
- Rutas a los archivos de una carpeta específica:
 - La máscara "C:\dir*.*" comprende las rutas a todos los archivos de la carpeta C:\dir\, pero no a los de las subcarpetas de C:\dir\.
 - La máscara "C:\dir*" comprende las rutas a todos los archivos de la carpeta C:\dir\, pero no a los de las subcarpetas de C:\dir\.
 - La máscara "C:\dir\" comprende las rutas a todos los archivos de la carpeta C:\dir\, pero no a los de las subcarpetas de C:\dir\.
 - La máscara "C:\dir*.exe" comprende las rutas a todos los archivos de extensión EXE almacenados en C:\dir\, pero no a los de las subcarpetas de C:\dir\.
 - La máscara "C:\dir\prueba" comprende las rutas a todos los archivos de nombre "prueba" almacenados en C:\dir\, pero no a los almacenados en las subcarpetas de C:\dir\.
 - La máscara "C:\dir*\prueba" comprende las rutas a todos los archivos de nombre "prueba" almacenados en C:\dir\ y en las subcarpetas de C:\dir\.
- Rutas a los archivos de cualquier carpeta que tenga un nombre específico:

- La máscara "dir*.*" comprende todas las rutas a archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara "dir*" comprende las rutas a todos los archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara "dir\" comprende las rutas a todos los archivos almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara "dir*.exe" comprende las rutas a todos los archivos de extensión EXE almacenados en carpetas de nombre "dir", pero no a los que se encuentran en subcarpetas de esas carpetas.
- La máscara "dir\prueba" comprende las rutas a todos los archivos de nombre "prueba" almacenados en carpetas de nombre "dir", pero no a los almacenados en subcarpetas de esas carpetas.

d. En la ventana **Nombre de archivo o carpeta**, haga clic en **Aceptar**.

Aparece un enlace al archivo o carpeta agregados en la sección **Descripción de la exclusión del análisis** de la ventana **Exclusión del análisis**.

6. Para excluir objetos que tengan un nombre específico del análisis:

a. En la sección **Propiedades**, seleccione la casilla de verificación **Nombre de objeto**.

b. Haga clic en el enlace **Introducir un nombre de objeto** de la sección **Descripción de la exclusión del análisis** para abrir la ventana **Nombre de objeto**.

c. Introduzca el nombre del objeto o la máscara del nombre según la clasificación de la Enciclopedia del virus de Kaspersky:

d. Haga clic en **Aceptar** en la ventana **Nombre de objeto**.

Aparece un enlace al nombre del objeto agregado en la sección **Descripción de la exclusión del análisis** de la ventana **Exclusión del análisis**.

7. Si es preciso, en el campo **Comentario**, introduzca un breve comentario sobre la exclusión del análisis que va a crear.

8. Especifique los componentes de Kaspersky Endpoint Security que van a emplearse en la exclusión del análisis:

a. Haga clic en el enlace **Todos** de la sección **Descripción de la exclusión del análisis** para abrir el enlace **Seleccionar componentes**.

b. Haga clic en el enlace **Seleccionar componentes** para abrir la ventana **Componentes de protección**.

c. Seleccione las casillas de verificación situadas junto a los componentes a los cuales se debe aplicar la exclusión del análisis.

d. En la ventana **Componentes de protección**, haga clic en **Aceptar**.

Si se especifican los componentes en la configuración de la exclusión del análisis, dicha exclusión se aplica solo durante el análisis realizado por estos componentes de Kaspersky Endpoint Security.

Si no se especifican los componentes en la configuración de la exclusión del análisis, dicha exclusión se aplica durante el análisis realizado por todos los componentes de Kaspersky Endpoint Security.

9. En la ventana **Exclusión del análisis**, haga clic en **Aceptar**.

La exclusión del análisis que ha agregado aparece en la tabla en la pestaña **Exclusiones del análisis** de la ventana **Zona de confianza**. Los parámetros configurados de esta exclusión del análisis aparecen en la sección **Descripción de la exclusión del análisis**.

10. En la ventana **Zona de confianza**, haga clic en **Aceptar**.
11. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Modificación de una exclusión del análisis

Para modificar una exclusión del análisis:

1. Abra la [ventana de configuración de la aplicación](#).
2. Seleccione la sección **Protección Antivirus** situada a la izquierda.
La configuración de la protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.
Se abre la ventana **Zona de confianza** en la pestaña **Exclusiones del análisis**.
4. Seleccione la exclusión del análisis que desea modificar en la lista.
5. Cambie la configuración de la exclusión del análisis mediante uno de los siguientes métodos:
 - Haga clic en el botón **Modificar**.
Se abre la ventana **Exclusiones del análisis**.
 - Abra la ventana para editar el ajuste necesario haciendo clic en el enlace en el campo **Descripción de la exclusión del análisis**.
6. Si hizo clic en el botón **Editar** durante el paso anterior, haga clic en **Aceptar** en la ventana **Exclusión del análisis**.
La configuración modificada de esta exclusión del análisis aparece en la sección **Descripción de la exclusión del análisis**.
7. En la ventana **Zona de confianza**, haga clic en **Aceptar**.
8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Eliminación de una exclusión del análisis

Para eliminar una exclusión del análisis:

1. Abra la [ventana de configuración de la aplicación](#).
2. Seleccione la sección **Protección Antivirus** situada a la izquierda.
La configuración de la protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.
Se abre la ventana **Zona de confianza** en la pestaña **Exclusiones del análisis**.

4. Seleccione la exclusión del análisis que necesita en la lista de exclusiones del análisis.
5. Haga clic en el botón **Eliminar**.
La exclusión del análisis eliminada desaparece de la lista.
6. En la ventana **Zona de confianza**, haga clic en **Aceptar**.
7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Activación y desactivación de una exclusión del análisis

Para activar o desactivar una exclusión del análisis:

1. Abra la [ventana de configuración de la aplicación](#).
2. Seleccione la sección **Protección Antivirus** situada a la izquierda.
La configuración de la protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.
Se abre la ventana **Zona de confianza** en la pestaña **Exclusiones del análisis**.
4. Seleccione la exclusión que necesita en la lista de exclusiones del análisis.
5. Realice una de las siguientes acciones:
 - Para activar una exclusión del análisis, seleccione la casilla de verificación situada junto al nombre de dicha exclusión del análisis.
 - Para desactivar una exclusión del análisis, desactive la casilla de verificación situada junto al nombre de dicha exclusión del análisis.
6. Haga clic en **Aceptar**.
7. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Edición de la lista de aplicaciones de confianza

Para editar la lista de aplicaciones de confianza:

1. Abra la [ventana de configuración de la aplicación](#).
2. Seleccione la sección **Protección Antivirus** situada a la izquierda.
La configuración de la protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.
Se abre la ventana **Zona de confianza**.
4. En la ventana **Zona de confianza**, seleccione la pestaña **Aplicaciones de confianza**.

5. Para agregar una aplicación a la lista de aplicaciones de confianza:

a. Haga clic en el botón **Agregar**.

b. En el menú contextual que se abre, lleve a cabo una de las siguientes acciones:

- Si desea encontrar la aplicación en la lista de las que están instaladas en el equipo, seleccione el elemento **Aplicaciones** en el menú.

Se abre la ventana **Seleccionar aplicación**.

- Si desea especificar la ruta del archivo ejecutable de la aplicación en cuestión, seleccione **Examinar**.

Se abre la ventana estándar **Abrir archivo** de Microsoft Windows.

c. Seleccione la aplicación de una de las siguientes formas:

- Si seleccionó **Aplicaciones** durante el paso anterior, seleccione la aplicación en la lista de aplicaciones instaladas en el equipo y haga clic en **Aceptar** en la ventana **Seleccionar aplicación**.

- Si seleccionó **Examinar** durante el paso anterior, especifique la ruta al archivo ejecutable de la aplicación correspondiente y haga clic en el botón **Abrir** de la ventana **Abrir** estándar de Microsoft Windows.

Estas acciones hacen que se abra la ventana **Exclusiones del análisis para la aplicación**.

a. Seleccione las casillas de verificación situadas junto a las reglas de la zona de confianza correspondientes a la aplicación seleccionada:

- **No analizar archivos abiertos.**
- **No supervisar la actividad de la aplicación.**
- **No heredar restricciones del proceso principal (aplicación).**
- **No vigilar la actividad de las subaplicaciones.**
- **No bloquear la interacción con la interfaz de la aplicación.**
- **No analizar el tráfico de red.**

b. En la ventana **Exclusiones del análisis para la aplicación**, haga clic en **Aceptar**.

La aplicación de confianza que ha agregado aparece en la lista de aplicaciones de confianza.

6. Para editar la configuración de una aplicación de confianza:

a. Seleccione una aplicación en la lista de aplicaciones de confianza.

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

c. Se abre la ventana **Exclusiones del análisis para la aplicación**.

d. Seleccione o desactive las casillas de verificación situadas junto a las reglas de la zona de confianza correspondientes a la aplicación seleccionada:

Si no se seleccionan reglas de zona de confianza en la ventana **Exclusiones del análisis para la aplicación**, la [aplicación de confianza se incluye en el análisis](#). En este caso, la aplicación de confianza no se elimina de la lista de aplicaciones de confianza, pero se desactiva su casilla de verificación.

- e. En la ventana **Exclusiones del análisis para la aplicación**, haga clic en **Aceptar**.
7. Para quitar una aplicación de la lista de aplicaciones de confianza:
 - a. Seleccione una aplicación en la lista de aplicaciones de confianza.
 - b. Haga clic en el botón **Eliminar**.
8. En la ventana **Zona de confianza**, haga clic en **Aceptar**.
9. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Activación y desactivación de reglas de la zona de confianza para una aplicación en la lista de aplicaciones de confianza

Para activar o desactivar la acción de las reglas de la zona de confianza aplicadas a una aplicación de la lista de aplicaciones de confianza:

1. Abra la [ventana de configuración de la aplicación](#).
2. Seleccione la sección **Protección Antivirus** situada a la izquierda.

La configuración de la protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.

Se abre la ventana **Zona de confianza**.
4. En la ventana **Zona de confianza**, seleccione la pestaña **Aplicaciones de confianza**.
5. En la lista de aplicaciones de confianza, seleccione la aplicación de confianza necesaria.
6. Realice una de las siguientes acciones:
 - Para excluir una aplicación de confianza del análisis de Kaspersky Endpoint Security, seleccione la casilla de verificación situada junto a su nombre.
 - Para incluir excluir una aplicación de confianza en el análisis de Kaspersky Endpoint Security, desactive la casilla de verificación situada junto a su nombre.
7. Haga clic en **Aceptar**.
8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Uso del almacén de certificados de confianza del sistema

El uso del almacén de certificados del sistema le permite excluir aplicaciones firmadas por una firma digital de confianza del análisis de virus. A continuación, Kaspersky Endpoint Security asigna la aplicación al *grupo de confianza* apropiado.

Para comenzar a utilizar el almacén de certificados de confianza del sistema:

1. Abra la [ventana de configuración de la aplicación](#).
2. Seleccione la sección **Protección Antivirus** situada a la izquierda.
La configuración de la protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.
Se abre la ventana **Zona de confianza**.
4. En la ventana **Zona de confianza**, seleccione la pestaña **Almacén de confianza de certificados del sistema**.
5. Seleccione la casilla de verificación **Usar almacén de confianza de certificados del sistema**.
6. En la lista desplegable **Almacén de confianza de certificados del sistema**, seleccione qué almacén del sistema de Kaspersky Endpoint Security se debe considerar como de confianza.
7. En la ventana **Zona de confianza**, haga clic en **Aceptar**.
8. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Autoprotección de Kaspersky Endpoint Security

Esta sección describe los mecanismos de autoprotección y protección de control remoto de Kaspersky Endpoint Security y proporciona instrucciones sobre la configuración de los parámetros de estos mecanismos.

Acerca de la Autoprotección de Kaspersky Endpoint Security

Kaspersky Endpoint Security protege al equipo frente a programas maliciosos, entre los que se incluye el software malicioso (malware), que intenta bloquear el funcionamiento de Kaspersky Endpoint Security o incluso eliminarlo del equipo.

La estabilidad del sistema de seguridad en el equipo se garantiza a través de la autoprotección y los mecanismos de protección mediante control remoto en Kaspersky Endpoint Security.

El mecanismo *Autoprotección* impide la modificación o eliminación de los archivos de las aplicaciones del disco duro, los procesos de la memoria y las entradas del registro del sistema.

Protección de control remoto bloquea todos los intentos de un equipo remoto de controlar los servicios de las aplicaciones.

En los equipos que se ejecutan con sistemas operativos de 64 bits, solo está disponible la Autoprotección de Kaspersky Endpoint Security para impedir la modificación y la eliminación de los archivos de aplicaciones en las entradas del Registro del sistema y el disco duro.

Activación y desactivación de la Autoprotección

El mecanismo de autoprotección de Kaspersky Endpoint Security está activado de forma predeterminada. Si es necesario, puede desactivar la Autoprotección.

Para habilitar o deshabilitar Autoprotección, haga lo siguiente:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.
3. Realice una de las siguientes acciones:
 - Para habilitar el mecanismo de autoprotección, active la casilla de verificación **Activar la Autoprotección**.
 - Para deshabilitar el mecanismo de autoprotección, desactive la casilla de verificación **Activar la Autoprotección**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Activación o desactivación de Protección de control remoto

El mecanismo de protección de control remoto está activado de forma predeterminada. Puede desactivar el mecanismo de protección de control remoto, si fuera necesario.

Para activar o desactivar el mecanismo de protección de control remoto:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.
3. Realice una de las siguientes acciones:
 - Para activar el mecanismo de protección de control remoto, seleccione **Desactivar gestión externa del servicio del sistema**.
 - Para desactivar el mecanismo de protección de control remoto, borre **Desactivar gestión externa del servicio del sistema**.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Soporte de las aplicaciones de administración remota

Puede que alguna que otra vez necesite usar una aplicación de administración remota mientras está activada la protección por control externo.

Para activar el funcionamiento de las aplicaciones de administración remota:

1. Abra la [ventana de configuración de la aplicación](#).
2. Seleccione la sección **Protección Antivirus** situada a la izquierda.
La configuración de la protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Exclusiones de análisis y aplicaciones de confianza**, haga clic en el botón **Configuración**.
Se abre la ventana **Zona de confianza**.
4. En la ventana **Zona de confianza**, seleccione la pestaña **Aplicaciones de confianza**.
5. Haga clic en el botón **Agregar**.
6. En el menú contextual que se abre, lleve a cabo una de las siguientes acciones:
 - Para encontrar la aplicación de administración remota en la lista de las que están instaladas en el equipo, seleccione el elemento **Aplicaciones**.
Se abre la ventana **Seleccionar aplicación**.
 - Para especificar la ruta del archivo ejecutable de la aplicación de administración remota, seleccione **Examinar**.
Se abre la ventana estándar **Abrir archivo** de Microsoft Windows.
7. Seleccione la aplicación de una de las siguientes formas:
 - Si seleccionó **Aplicaciones** durante el paso anterior, seleccione la aplicación en la lista de aplicaciones instaladas en el equipo y haga clic en **Aceptar** en la ventana **Seleccionar aplicación**.
 - Si seleccionó **Examinar** durante el paso anterior, especifique la ruta al archivo ejecutable de la aplicación correspondiente y haga clic en el botón **Abrir** de la ventana **Abrir** estándar de Microsoft Windows.Estas acciones hacen que se abra la ventana **Exclusiones del análisis para la aplicación**.
8. Seleccione la casilla de verificación **No supervisar la actividad de la aplicación**.
9. En la ventana **Exclusiones del análisis para la aplicación**, haga clic en **Aceptar**.
La aplicación de confianza que ha agregado aparece en la lista de aplicaciones de confianza.
10. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Rendimiento de Kaspersky Endpoint Security y compatibilidad con otras aplicaciones

Esta sección contiene información sobre el rendimiento de Kaspersky Endpoint Security y la compatibilidad con otras aplicaciones, así como pautas para seleccionar los tipos de objetos que se pueden detectar y el modo de funcionamiento de Kaspersky Endpoint Security.

Acerca de rendimiento de Kaspersky Endpoint Security y compatibilidad con otras aplicaciones

Rendimiento de Kaspersky Endpoint Security

El rendimiento de Kaspersky Endpoint Security se refiere al número de tipos de objetos que puedan dañar el equipo que son detectables, así como al consumo de energía y uso de los recursos del equipo.

Selección de los tipos de objetos detectables

Kaspersky Endpoint Security le permite ajustar la protección de su equipo y seleccionar los [tipos de objetos](#) que la aplicación detecta durante su funcionamiento. Kaspersky Endpoint Security el sistema operativo en busca de virus, gusanos y troyanos. No puede desactivar el análisis de estos tipos de objetos. Este tipo de software malicioso (malware) puede provocar daños significativos en el equipo. Para lograr una mayor protección en su equipo, puede ampliar la gama de tipos de objetos detectables si activa el control de software legal que pueden usar los delincuentes para dañar su equipo o sus datos personales.

Uso del modo de ahorro de energía

El consumo de energía que hacen las aplicaciones es un aspecto básico para los equipos portátiles. Por lo general, las tareas planificadas de Kaspersky Endpoint Security consumen una gran cantidad de recursos. Cuando un equipo se está ejecutando con alimentación de la batería, puede usar el modo de ahorro de energía para moderar su consumo.

En el modo de ahorro de energía, se posponen automáticamente las siguientes tareas planificadas:

- [Tarea de actualización](#)
- [Tarea Análisis completo](#)
- [Tarea de Análisis de áreas críticas](#)
- [Tarea de análisis personalizado](#)
- [Tarea Análisis de vulnerabilidades](#)
- [Tarea Comprobación de integridad](#)

Independientemente de si el modo de ahorro de energía está activado o no, Kaspersky Endpoint Security suspende las tareas de cifrado cuando el portátil cambia al funcionamiento con batería. La aplicación reanuda las tareas de cifrado cuando el portátil cambia del funcionamiento con batería al funcionamiento por red eléctrica.

Concesión de recursos del equipo a otras aplicaciones

El uso que hace Kaspersky Endpoint Security de los recursos del equipo puede afectar al rendimiento de otras aplicaciones. Para solucionar el problema del funcionamiento simultáneo durante el aumento de la carga en los subsistemas del disco duro y la CPU, Kaspersky Endpoint Security puede suspender las tareas planificadas y asignar recursos a otras aplicaciones.

No obstante, diversas aplicaciones se ejecutan inmediatamente cuando los recursos de la CPU pasan a estar disponibles y siguen funcionando en segundo plano. Para evitar que el análisis dependa del rendimiento de otras aplicaciones, es recomendable no conceder a dichas aplicaciones recursos del sistema operativo.

Si es necesario, puede iniciar dichas tareas manualmente.

Uso de tecnología de desinfección avanzada

Los programas maliciosos actuales pueden penetrar en los niveles más bajos del sistema operativo, lo que los hace prácticamente imposibles de eliminar. Tras la detección de actividad maliciosa en el sistema operativo, Kaspersky Endpoint Security lleva a cabo un proceso de desinfección exhaustiva por medio de la [tecnología de desinfección avanzada](#). El objetivo de la *tecnología de desinfección avanzada* consiste en eliminar del sistema operativo los programas maliciosos que ya han puesto en marcha sus procesos en la memoria RAM y que impiden que Kaspersky Endpoint Security los elimine por medio de otros métodos. Como consecuencia de ello, se neutraliza la amenaza. Cuando la desinfección avanzada está en curso, se recomienda que no ponga en marcha ningún proceso nuevo ni modifique el registro del sistema operativo. La tecnología de desinfección avanzada emplea un número considerable de recursos del sistema operativo, lo que puede ralentizar el resto de las aplicaciones.

Después de que la desinfección avanzada haya finalizado en un equipo que ejecuta con Microsoft Windows para estaciones de trabajo, Kaspersky Endpoint Security solicita el permiso del usuario para reiniciar el equipo. Después del reinicio del sistema, Kaspersky Endpoint Security elimina los archivos de software malicioso e inicia un "pequeño" análisis completo del equipo.

Resulta imposible que se solicite el reinicio en un equipo que se ejecuta con Microsoft Windows para servidores de archivos debido a las especificaciones de Kaspersky Endpoint Security para servidores de archivos. El reinicio de un servidor de archivos no planificado puede conllevar problemas que impliquen la no disponibilidad temporal de los datos del servidor de archivos o la pérdida de datos no guardados. Se recomienda reiniciar el servidor de archivos únicamente de acuerdo con la planificación. Esta es la razón por la cual la tecnología de desinfección avanzada está [desactivada](#) de forma predeterminada para los servidores de archivos.

Si se detecta una infección activa en un servidor de archivos, se envía a Kaspersky Security Center un evento con información que indica que se debe realizar la desinfección activa. Para desinfectar la infección activa de un servidor de archivos, active la tecnología de desinfección activa para servidores de archivos e inicie una tarea de grupo de *Análisis antivirus* en el momento que resulte adecuado para los usuarios del servidor del archivo.

Selección de los tipos de objetos detectables

Para seleccionar los tipos de objetos detectables:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, seleccione la sección **Protección antivirus**.
La configuración de la protección antivirus se muestra en la parte derecha de la ventana.
3. En la sección **Objetos**, haga clic en el botón **Configuración**.
Se abre la ventana **Objetos para la detección**.
4. Seleccione las casillas de verificación de los tipos de objetos que desea que Kaspersky Endpoint Security detecte:
 - **Herramientas maliciosas**
 - **Software publicitario**

- **Marcadores automáticos (auto-dialers)**
- **Otro**
- **Archivos empaquetados que pueden causar daños**
- **Archivos comprimidos varias veces**

5. Haga clic en **Aceptar**.

Se cierra la ventana **Objetos para la detección**. En la sección **Objetos**, se muestran los tipos de objetos seleccionados en **Está activada la detección de los siguientes tipos de objetos**.

6. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Activación o desactivación de la tecnología de desinfección avanzada de estaciones de trabajo

Para activar o desactivar la tecnología de desinfección avanzada de estaciones de trabajo:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, seleccione la sección **Protección antivirus**.
La configuración de la protección antivirus se muestra en la parte derecha de la ventana.
3. En la parte derecha de la ventana, seleccione una de las siguientes acciones:
 - Seleccione **Activar tecnología de desinfección avanzada** para activar la tecnología de desinfección avanzada.
 - Desactive **Activar tecnología de desinfección avanzada** para desactivar la tecnología de desinfección avanzada.
4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Si la tarea de desinfección avanzada se inicia a través de Kaspersky Security Center, la mayoría de funciones del sistema operativo no estarán disponibles para el usuario. La estación de trabajo se reinicia después de completarse la tarea.

Activación o desactivación de la tecnología de desinfección avanzada de servidores de archivos

Para activar la tecnología de desinfección avanzada de servidores de archivos, realice una de las siguientes acciones:

- Active la tecnología de desinfección avanzada en las propiedades de la directiva de Kaspersky Security Center activa. Para ello:
 - a. Abra la sección **Configuración general de protección** en la ventana de propiedades de la directiva.

- b. Seleccione la casilla de verificación **Activar tecnología de desinfección avanzada**.
- c. Para guardar los cambios, haga clic en **Aceptar** en la ventana de propiedades de la directiva.
- En las propiedades de la tarea de grupo Análisis antivirus de Kaspersky Security Center, seleccione la casilla de verificación **Ejecutar la desinfección avanzada de inmediato**.

Para desactivar la tecnología de desinfección avanzada de servidores de archivos, realice una de las siguientes acciones:

- Active la tecnología de desinfección avanzada en las propiedades de la directiva de Kaspersky Security Center. Para ello:
 - a. Abra la sección **Configuración general de protección** en la ventana de propiedades de la directiva.
 - b. Desactive la casilla de verificación **Activar tecnología de desinfección avanzada**.
 - c. Para guardar los cambios, haga clic en **Aceptar** en la ventana de propiedades de la directiva.
- En las propiedades de la tarea de grupo Análisis antivirus de Kaspersky Security Center, desactive la casilla de verificación **Ejecutar la desinfección avanzada de inmediato**.

Activación o desactivación del modo de ahorro de energía

Para activar o desactivar el modo de conservación de energía:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Modo de funcionamiento**, haga clic en el botón **Configuración**.
Se abre la ventana **Modo de funcionamiento**.
4. Lleve a cabo las siguientes acciones en la ventana **Modo de funcionamiento**:
 - Para activar el modo de conservación de energía, seleccione la casilla de verificación **Desactivar tareas planificadas mientras funciona con la batería**.
Cuando se activa el modo de conservación de energía y el equipo funciona con la energía de la batería, las tareas siguientes no se ejecutan aunque estén planificadas:
 - Tarea de actualización
 - Tarea Análisis completo
 - Tarea de Análisis de áreas críticas
 - Tarea de análisis personalizado
 - Tarea Análisis de vulnerabilidades
 - Tarea Comprobación de integridad

- Si desea desactivar el modo de conservación de energía, desactive la casilla de verificación **Posponer tareas planificadas mientras funciona con la batería**. En este caso, Kaspersky Endpoint Security lleva a cabo las tareas planificadas independientemente de la fuente de energía del equipo.

5. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Activación o desactivación de la concesión de recursos a otras aplicaciones

Para activar o desactivar la concesión de recursos a otras aplicaciones:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.

La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.

3. En la sección **Modo de funcionamiento**, haga clic en el botón **Configuración**.

Se abre la ventana **Modo de funcionamiento**.

4. Lleve a cabo las siguientes acciones en la ventana **Modo de funcionamiento**:

- Si desea activar el modo según el cual se conceden recursos a otras aplicaciones, seleccione la casilla de verificación **Facilitar recursos para otras aplicaciones**.

Cuando se configura la concesión de recursos a otras aplicaciones, Kaspersky Endpoint Security pospone las tareas planificadas que ralentizan a otras aplicaciones:

- Tarea de actualización
 - Tarea Análisis completo
 - Tarea de Análisis de áreas críticas
 - Tarea de análisis personalizado
 - Tarea Análisis de vulnerabilidades
 - Tarea Comprobación de integridad
- Si desea desactivar el modo según el cual se conceden recursos a otras aplicaciones, desactive la casilla de verificación **Facilitar recursos para otras aplicaciones**. En este caso, Kaspersky Endpoint Security lleva a cabo las tareas planificadas independientemente del funcionamiento de otras aplicaciones.

De forma predeterminada, la aplicación está configurada para conceder recursos a otras aplicaciones.

5. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Protección con contraseña

Esta sección contiene información sobre el acceso restringido a Kaspersky Endpoint Security con una contraseña.

Acerca del acceso restringido a Kaspersky Endpoint Security

Varios usuarios con distintos niveles de conocimientos informáticos pueden usar un solo equipo. Si los usuarios cuentan con acceso ilimitado a Kaspersky Endpoint Security y su configuración, el nivel general de protección del equipo puede verse reducido.

Puede restringir el acceso a Kaspersky Endpoint Security mediante la configuración de un nombre de usuario y una contraseña y la especificación de operaciones para las que la aplicación solicita dichas credenciales al usuario:

Cuando se actualiza una versión anterior de la aplicación a Kaspersky Endpoint Security 10 Service Pack 2 para Windows, la contraseña se preserva (si se había definido). Para modificar la configuración de protección con contraseña por primera vez, use el nombre de usuario predeterminado KLAdmin.

Activación y desactivación de la protección con contraseña

Se recomienda ser precavido a la hora de usar una contraseña para restringir el acceso a la aplicación. Si ha olvidado la contraseña, [póngase en contacto con el Soporte técnico de Kaspersky](#) para obtener instrucciones sobre la eliminación de la protección con contraseña.

Para activar la protección con contraseña:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
La configuración de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Protección con contraseña**, haga clic en el botón **Configuración**.
Se abre la ventana **Protección con contraseña**.
4. Seleccione la casilla de verificación **Activar la protección con contraseña**.
5. En el campo **Nombre de usuario**, introduzca el nombre de usuario que se debe especificar en la ventana **Comprobación de la contraseña** cuando se realicen las siguientes operaciones protegidas con contraseña.
6. En el campo **Nueva contraseña**, introduzca una contraseña para acceder a la aplicación.
7. Confirme la contraseña en el campo **Confirme contraseña**.
8. Si desea restringir el acceso a todas las operaciones con la aplicación, en la sección **Cobertura de la contraseña**, haga clic en el botón **Seleccionar todo**.
9. Si desea restringir selectivamente el acceso del usuario, en la sección **Cobertura de la contraseña**, seleccione las casillas de verificación que hay junto a los nombres de las operaciones relevantes:
 - **Configurar aplicación.**
 - **Salir de la aplicación.**

- Desactivar componentes de protección.
- Desactivar componentes de control.
- Quitar clave.
- Eliminar/modificar/restaurar la aplicación.
- Restaurar el acceso a los datos en las unidades cifradas.
- Visualizar informes.

10. Haga clic en el botón **Aceptar**.

La aplicación comprobará que se han introducido las contraseñas: Si las contraseñas coinciden, la aplicación usa la contraseña. Si las contraseñas no coinciden, la aplicación le solicitará que confirme la contraseña de nuevo en el campo **Confirmar contraseña**.

Una vez que la protección con contraseña esté activada, la aplicación solicitará una contraseña cada vez que se realice una operación incluida en la cobertura de la contraseña. Si no desea que la aplicación le solicite la contraseña cada vez que intente realizar una operación protegida con contraseña durante la sesión actual, seleccione la casilla de verificación **Guardar contraseña para esta sesión** en la ventana **Comprobación de contraseña**.

Al desactivar la casilla de verificación **Guardar contraseña para esta sesión**, la aplicación le solicita que introduzca la contraseña cada vez que intente realizar una operación protegida con contraseña.

Para desactivar la protección con contraseña:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
La configuración de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Protección con contraseña**, haga clic en el botón **Configuración**.
Se abre la ventana **Protección con contraseña**.
4. Desactive la casilla de verificación **Activar la protección con contraseña**.

Para desactivar la protección con contraseña, deberá iniciar sesión con el usuario KLAdmin. La protección con contraseña no puede desactivarse cuando se está usando una contraseña temporal o cualquier otra cuenta.

5. Haga clic en el botón **Aceptar**.

Una vez que la protección con contraseña está desactivada, el acceso restringido a la aplicación se cancelará la próxima vez que se inicie Kaspersky Endpoint Security.

Modificación de la contraseña de acceso a Kaspersky Endpoint Security

Para modificar la contraseña de acceso a Kaspersky Endpoint Security:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
3. En la sección **Protección con contraseña**, haga clic en el botón **Configuración**.
Se abre la ventana **Protección con contraseña**.
4. Introduzca el nombre de usuario en el campo **Nombre de usuario**.
5. En el campo **Nueva contraseña**, introduzca una nueva contraseña para acceder a la aplicación.
6. En el campo **Confirmar contraseña**, vuelva a introducir la nueva contraseña.
7. Haga clic en **Aceptar**.

La aplicación comprobará que se han introducido las contraseñas: Si las contraseñas coinciden, la aplicación aplicará la nueva contraseña y se cerrará la ventana **Protección con contraseña**. Si las contraseñas no coinciden, la aplicación le solicitará que confirme la contraseña de nuevo en el campo **Confirmar contraseña**.

8. Para guardar los cambios realizados, en la ventana de configuración de la aplicación, haga clic en el botón **Guardar**.

Acerca de la utilización de una contraseña temporal

Cuando trabajan en equipos cliente administrados por una directiva de Kaspersky Security Center, es posible que los usuarios deban realizar operaciones con Kaspersky Endpoint Security protegidas con contraseña a nivel de directiva. Cuando se activa la protección con contraseña, únicamente el administrador de Kaspersky Security Center puede realizar las operaciones especificadas en el alcance de la contraseña. Sin embargo, si la conexión con Kaspersky Security Center se ha perdido (por ejemplo, cuando el usuario está fuera de la red corporativa), se limitan las funciones para trabajar con la interfaz local de Kaspersky Security Center.

Para proporcionar a un usuario la posibilidad de realizar las operaciones necesarias sin dar al usuario la contraseña que está definida en la configuración de la directiva, el administrador de Kaspersky Security Center puede crear una contraseña temporal. Una contraseña temporal tiene un período de validez y una cobertura de acción limitados. Después de que el usuario introduzca la contraseña temporal en la interfaz local de la aplicación, las operaciones permitidas por el administrador de Kaspersky Security Center pasarán a estar disponibles.

Cuando la contraseña temporal caduca, Kaspersky Endpoint Security continúa funcionando de acuerdo con la configuración de la directiva de Kaspersky Security Center. Las operaciones protegidas con contraseña a nivel de la directiva dejan de estar disponibles para el usuario.

Crear una contraseña temporal utilizando la consola de administración de Kaspersky Security Center

Para crear una contraseña temporal y enviarla a un usuario:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta con el nombre del grupo de administración que incluye el equipo del usuario que solicita la contraseña temporal.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. En el menú contextual del equipo que pertenece al usuario que solicita la contraseña temporal, seleccione **Propiedades**.

Se abre la ventana **Propiedades: <Nombre del equipo>**.

5. En la ventana **Propiedades: <nombre del equipo>**, seleccione la sección **Aplicaciones**.
6. Seleccione Kaspersky Endpoint Security Service Pack 2 para Windows y abra la ventana de propiedades de la aplicación mediante uno de los siguientes métodos:
 - Haga clic en el botón **Propiedades** situado en la parte inferior de la pantalla.
 - En el menú contextual de la aplicación, seleccione **Propiedades**.

Esto abre la ventana **Configuración de la aplicación "<Nombre de la aplicación>"**.

7. En la ventana **Configuración de la aplicación "<Nombre de la aplicación>"**, en la sección **Configuración avanzada**, seleccione el apartado **Configuración de la aplicación**.
8. En la sección **Protección con contraseña**, haga clic en el botón **Configuración**.
Se abre la ventana **Protección con contraseña**.
9. En la ventana **Protección con contraseña**, en la sección **Contraseña temporal**, haga clic en el botón **Configuración**.

Este botón está disponible si se activa la protección con contraseña para Kaspersky Security Center en la directiva de Kaspersky Security Center que se está ejecutando en el equipo.

Se abre la ventana **Crear contraseña temporal**.

10. En el campo **Fecha de caducidad**, especifique la fecha en la cual el usuario ya no podrá utilizar la contraseña temporal.
En esta fecha, la contraseña temporal dejará de ser válida. Se debe crear una nueva contraseña temporal para proporcionar acceso a la realización de operaciones en la interfaz local de Kaspersky Endpoint Security.
11. En la tabla **Cobertura de la contraseña temporal**, seleccione las casillas de verificación situadas junto a las operaciones que deben estar disponibles para el usuario mientras la contraseña temporal sea válida.
12. Haga clic en el botón **Crear**.
Esto abre la ventana **Contraseña temporal** que contiene una contraseña cifrada.
13. Copie la contraseña y las [instrucciones sobre cómo aplicarla](#) y envíesela al usuario.

Aplicar una contraseña temporal en la interfaz de Kaspersky Endpoint Security

Estas instrucciones están destinadas a los usuarios de equipos cliente donde se haya instalado Kaspersky Endpoint Security.

Para aplicar una contraseña temporal:

1. Abra la [ventana de configuración de la aplicación](#).

2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
La configuración de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Protección con contraseña**, haga clic en el botón **Contraseña temporal**.
Se abre la ventana **Contraseña temporal**.
4. Seleccione la casilla de verificación **Activar contraseña temporal**.
5. En el campo de entrada, especifique la contraseña que proporcionó el administrador de Kaspersky Security Center.
6. Haga clic en **Aceptar** para guardar los cambios.

Tras aplicar la contraseña temporal, las operaciones especificadas por el administrador de Kaspersky Security Center pasarán a estar disponibles. La ventana **Contraseña temporal** muestra la fecha de caducidad de la contraseña temporal y las operaciones permitidas.

Administración remota de la aplicación con Kaspersky Security Center

Esta sección describe la administración de Kaspersky Endpoint Security a través de Kaspersky Security Center.

Acerca de la administración de la aplicación a través de Kaspersky Security Center

Kaspersky Security Center le permite, de forma remota, instalar y desinstalar e iniciar y detener Kaspersky Endpoint Security, configurar la configuración de la aplicación, cambiar el conjunto de componentes de aplicación disponibles, añadir claves e iniciar actualizaciones y tareas de análisis.

Para obtener información acerca de la gestión de la aplicación mediante Kaspersky Security Center que no se proporcione en este documento, consulte la *Guía de administrador de Kaspersky Security Center*.

La aplicación se puede administrar mediante Kaspersky Security Center utilizando el complemento de administración Kaspersky Endpoint Security.

La versión del complemento de administración puede diferir de la versión de Kaspersky Endpoint Security instalada en el equipo cliente. Si la versión instalada del complemento de administración tiene menos funcionalidad que la versión instalada de Kaspersky Endpoint Security, la configuración de las funciones ausentes no está regulada por el complemento de administración. El usuario puede modificar dicha configuración en la interfaz local de Kaspersky Endpoint Security.

Consideraciones especiales al trabajar con versiones diferentes de complementos de administración

Puede utilizar un complemento de administración para cambiar los siguientes elementos:

- Directivas
- Perfiles de directivas
- Tareas de grupo
- Tareas locales
- Configuración local de Kaspersky Endpoint Security

Puede administrar Kaspersky Endpoint Security mediante Kaspersky Security Center solo si dispone de un complemento de administración cuya versión es igual o más reciente que la versión especificada en la información con relación a la compatibilidad de Kaspersky Endpoint Security con el complemento de administración. Puede ver la versión mínima requerida del complemento de administración en el archivo `installer.ini` incluido en el [kit de distribución](#).

Si algún componente se abre, el complemento de administración comprueba su información de compatibilidad. Si la versión del complemento de administración es la misma o posterior a la versión especificada en la información de compatibilidad, puede cambiar la configuración de este componente. De lo contrario, no puede utilizar el complemento de administración para cambiar la configuración del componente seleccionado. Se recomienda actualizar el complemento de administración.

Cambiar la configuración anteriormente definida utilizando una versión posterior del complemento de administración

Puede utilizar una versión posterior del complemento de administración para cambiar toda la configuración definida anteriormente y configurar los nuevos ajustes que no estaban presentes en su versión anterior del complemento de administración.

Para los nuevos ajustes, una versión posterior del complemento de administración asigna los valores predeterminados cuando se guarda una directiva, perfil de directiva o tarea por primera vez.

Tras cambiar la configuración de una directiva, el perfil de una directiva o una tarea de grupo utilizando una versión posterior del complemento de administración, estos componentes dejarán de estar disponibles para versiones anteriores del complemento de administración. Los ajustes locales de Kaspersky Endpoint Security y los ajustes de las tareas locales siguen estando disponibles para el complemento de administración de versiones anteriores.

Ejecución y detención de Kaspersky Endpoint Security en un equipo cliente

Para iniciar o detener la aplicación en un equipo cliente, haga lo siguiente:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del [grupo de administración](#) al que pertenece el equipo cliente pertinente.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. Seleccione el equipo en el que desee ejecutar o detener la aplicación.
5. Haga clic con el botón derecho del ratón para que aparezca el menú contextual del equipo cliente y seleccione **Propiedades**.


Se abre una ventana de propiedades del equipo cliente.

6. En la ventana de propiedades del equipo cliente, seleccione la sección **Aplicaciones**.

Aparecerá una lista de las aplicaciones de Kaspersky que se han instalado en el equipo cliente en la parte derecha de la ventana de propiedades del equipo cliente.


7. Seleccione Kaspersky Endpoint Security 10 para Windows.

8. Haga lo siguiente:

- Para iniciar la aplicación, haga clic en el botón  situado a la derecha de la lista de aplicaciones de Kaspersky o haga lo siguiente:

- a. Seleccione **Propiedades** en el menú contextual de Kaspersky Endpoint Security o haga clic en el botón **Propiedades** que se encuentra bajo la lista de aplicaciones de Kaspersky.

Se abre la ventana **Configuración de la aplicación Kaspersky Endpoint Security 10 para Windows**.

- b. En la sección **General**, haga clic en el botón **Ejecutar** situado en la parte derecha de la ventana.
- Para detener la aplicación, haga clic en el botón  situado a la derecha de la lista de aplicaciones de Kaspersky o haga lo siguiente:
 - a. Seleccione **Propiedades** en el menú contextual de Kaspersky Endpoint Security o haga clic en el botón **Propiedades** que se encuentra bajo la lista de aplicaciones de Kaspersky.
Se abre la ventana **Configuración de la aplicación Kaspersky Endpoint Security 10 para Windows**.
 - b. En la sección **General**, haga clic en el botón **Detener**, que encontrará en la parte derecha de la ventana.

Configuración de los parámetros de Kaspersky Endpoint Security

Para configurar los parámetros de Kaspersky Endpoint Security haga lo siguiente:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del [grupo de administración](#) al que pertenece el equipo cliente pertinente.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. Seleccione el equipo para el que desee configurar los ajustes de Kaspersky Endpoint Security.
5. En el menú contextual del equipo cliente, seleccione **Propiedades**.
Se abre una ventana de propiedades del equipo cliente.
6. En la ventana de propiedades del equipo cliente, seleccione la sección **Aplicaciones**.
Aparecerá una lista de las aplicaciones de Kaspersky que se han instalado en el equipo cliente en la parte derecha de la ventana de propiedades del equipo cliente.
7. Seleccione la aplicación Kaspersky Endpoint Security 10 para Windows.
8. Realice una de las siguientes acciones:
 - Seleccione **Propiedades** en el menú contextual de Kaspersky Endpoint Security 10 para Windows.
 - Haga clic en el botón **Propiedades** que se encuentra bajo la lista de aplicaciones de Kaspersky.Se abre la ventana **Configuración de la aplicación Kaspersky Endpoint Security 10 para Windows**.
9. En la sección **Configuración avanzada**, configure los ajustes para Kaspersky Endpoint Security, así como los de informes y almacenes.

Las otras secciones de la ventana **Configuración de la aplicación Kaspersky Endpoint Security 10 para Windows** son las mismas que en las secciones de la aplicación estándar de Kaspersky Security Center. En la *Guía de administrador de Kaspersky Security Center* se proporciona una descripción de estas secciones.

Si una aplicación está sujeta a una directiva que prohíbe realizar cambios en los ajustes específicos, no podrá editarlos al configurar los ajustes de la aplicación en la sección **Configuración avanzada**.

10. Para guardar los cambios, en la ventana **Configuración de la aplicación Kaspersky Endpoint Security 10 para Windows**, haga clic en **Aceptar**.

Gestión de tareas

En esta sección, se describe la administración de tareas para Kaspersky Endpoint Security. Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la administración de tareas mediante Kaspersky Security Center.

Acerca de las tareas para Kaspersky Endpoint Security

Kaspersky Security Center controla la actividad de las aplicaciones de Kaspersky en equipos cliente mediante tareas. Las tareas implementan las principales funciones administrativas, como la instalación de claves, el análisis de equipos y la actualización de módulos de software de aplicaciones y bases de datos.

Puede crear los siguientes tipos de tareas para administrar Kaspersky Endpoint Security mediante Kaspersky Security Center:

- Tareas locales configuradas para un equipo cliente individual.
- Tareas de grupo configuradas para equipos cliente incluidos en grupos de administración.
- Tareas para un conjunto de equipos que no pertenecen a grupos de administración.

Las tareas para grupos de equipos que no pertenecen a grupos de administración solo se aplican a equipos cliente que se especifican en la configuración de tareas. Si se añaden nuevos equipos cliente a un grupo de equipos para el que se ha configurado una tarea, esta tarea no se aplica a estos nuevos equipos. Para aplicar la tarea a estos equipos, cree una nueva tarea o modifique la configuración de la tarea existente.

Para administrar Kaspersky Endpoint Security de forma remota, puede utilizar las siguientes tareas de cualquier de los tipos que se indican:

- **Agregar clave.** Kaspersky Endpoint Security agrega una clave para la activación de la aplicación, incluida una clave adicional.
- **Cambiar componentes de aplicación.** Kaspersky Endpoint Security instala o elimina componentes en equipos cliente según la lista de componentes especificados en la configuración de la tarea.
- **Inventario.** Kaspersky Endpoint Security recopila información acerca de todos los archivos ejecutables de las aplicaciones que se almacenan en los equipos.

Puede activar el inventario de módulos DLL y archivos de script. En este caso, Kaspersky Security Center recibirá información sobre módulos DLL cargados en un equipo con Kaspersky Endpoint Security instalado, así como sobre archivos que contienen scripts.

La activación del inventario de módulos DLL y archivos de script aumenta considerablemente la duración de la tarea de inventario y el tamaño de la base de datos.

- **Actualización.** Kaspersky Endpoint Security actualiza las bases de datos y los módulos de la aplicación en función de los parámetros de actualización configurados.
- **Deshacer.** Kaspersky Endpoint Security revierte la última actualización de bases de datos y módulos.
- **Análisis antivirus.** Kaspersky Endpoint Security analiza las áreas del equipo que se han especificado en la configuración de tareas para virus y otras amenazas.
- **Comprobación de conexión con KSN.** Kaspersky Endpoint Security envía una consulta sobre la disponibilidad de los servidores de KSN y actualiza el estado de conexión de KSN.
- **Comprobación de integridad.** Kaspersky Endpoint Security recibe datos sobre el conjunto de módulos de la aplicación instalados en el equipo cliente y analiza la firma digital de cada módulo.
- **Administrar cuentas del Agente de autenticación.** Al realizar esta tarea, Kaspersky Endpoint Security genera comandos para eliminar, agregar o modificar cuentas del Agente de autenticación.

Puede llevar a cabo las siguientes acciones mediante las tareas siguientes:

- Ejecutar, detener, suspender y reanudar tareas.
- Crear nuevas tareas.
- Modificar la configuración de tareas.

Los derechos de acceso a la configuración de las tareas de Kaspersky Endpoint Security (lectura, escritura, ejecución) se especifican para cada usuario que tenga acceso al servidor de administración de Kaspersky Security Center a través de la configuración del acceso a las áreas funcionales de Kaspersky Endpoint Security. Para configurar el acceso a las áreas funcionales de Kaspersky Endpoint Security, vaya a la sección **Seguridad** de la ventana de propiedades del servidor de administración de Kaspersky Security Center.

Configuración del modo de administración de tareas

Para configurar el modo de funcionamiento con tareas en la interfaz local de Kaspersky Endpoint Security:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta con el nombre del grupo de la administración para el cual desea configurar el modo de funcionamiento con tareas en la interfaz local de Kaspersky Endpoint Security.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.
6. En la sección **Configuración avanzada**, seleccione el apartado **Configuración de la aplicación**.
7. En la sección **Modo de funcionamiento**:

- Si desea permitir que los usuarios trabajen con tareas locales en la interfaz y la línea de comandos de Kaspersky Endpoint Security, seleccione la casilla de verificación **Permitir el uso de las tareas locales**.

Si la casilla de verificación se desactiva, las funciones de las tareas locales se detienen. De este modo, las tareas locales no se ejecutan según la planificación. Las tareas locales tampoco están disponibles para iniciar y editar en la interfaz local de Kaspersky Endpoint Security, ni tampoco con la línea de comandos.

- Si desea permitir que los usuarios vean la lista de tareas de grupo, seleccione la casilla de verificación **Permitir que las tareas de grupo se muestren**.
- Si desea permitir que los usuarios modifiquen la configuración de las tareas de grupo, seleccione la casilla de verificación **Permitir gestión de tareas de grupo**.

8. Para guardar los cambios, haga clic en el botón **Aceptar**.

9. Aplique la directiva.

Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información detallada sobre la aplicación de la directiva de Kaspersky Security Center.

Creación de una tarea local

Para crear una tarea local, haga lo siguiente:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del [grupo de administración](#) al que pertenece el equipo cliente pertinente.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. Seleccione el equipo para el cual desea crear una tarea local.
5. Realice una de las siguientes acciones:
 - En el menú contextual del equipo cliente, seleccione la opción **Todas las tareas** **Crear tarea**.
 - En el menú contextual del equipo cliente, seleccione **Propiedades** y, en la ventana **Propiedades: <Nombre del equipo>** que se abre, haga clic en el botón **Agregar** de la ficha **Tareas**.
 - En la lista desplegable **Realizar acción**, seleccione **Crear tarea**.

El Asistente de tareas comienza.

6. Siga las instrucciones del Asistente de tareas.

Creación de una tarea de grupos

Para crear una tarea de grupos, haga lo siguiente:

1. Abra la consola de administración de Kaspersky Security Center.
2. Realice una de las siguientes acciones:
 - Seleccione la carpeta **Dispositivos administrados** del árbol de la consola de administración a fin de crear una tarea de grupo para todos los equipos que administra Kaspersky Security Center.
 - En la carpeta **Dispositivos administrados** del árbol de la consola de administración, seleccione la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. Seleccione la pestaña **Tareas** del espacio de trabajo.
4. Haga clic en el botón **Crear tarea**.
El Asistente de tareas comienza.
5. Siga las instrucciones del Asistente de tareas.

Crear una tarea para selección de dispositivos

Para crear una tarea para la selección de dispositivos, realice lo siguiente:

1. Abra la consola de administración de Kaspersky Security Center.
2. Seleccione la carpeta **Tareas** en el árbol de la consola de administración.
3. Haga clic en el botón **Crear tarea**.
El Asistente de tareas comienza.
4. Siga las instrucciones del Asistente de tareas.
5. En la ventana **Seleccionar dispositivos a los que se asignará la tarea** del asistente, haga clic en el botón **Asignar tarea a una selección de dispositivos**.
6. En la siguiente ventana del Asistente, haga clic en el botón **Seleccionar**.
Se abre la ventana **Selección de dispositivos**.
7. Seleccione los dispositivos pertinentes.
8. Haga clic en **Aceptar** en la ventana **Selección de dispositivos**.
9. Siga las instrucciones del Asistente de tareas.

Ejecución, interrupción, suspensión y reanudación de una tarea

Si la aplicación de Kaspersky Endpoint Security [se ejecuta](#) en un equipo cliente, puede iniciar, detener, suspender y reanudar una tarea en este equipo cliente mediante Kaspersky Security Center. Cuando se suspende Kaspersky Endpoint Security, se suspenden las tareas en ejecución y resulta imposible ejecutar, detener, suspender o reanudar una tarea mediante Kaspersky Security Center.

Para ejecutar, detener, suspender o reiniciar una tarea local:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del [grupo de administración](#) al que pertenece el equipo cliente pertinente.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. Seleccione el equipo en el que desee iniciar, detener, suspender o reanudar una tarea local.
5. Haga clic con el botón derecho del ratón para que aparezca el menú contextual del equipo cliente y seleccione **Propiedades**.



Se abre una ventana de propiedades del equipo cliente.

6. Seleccione la sección **Tareas**.

Aparece una lista de tareas locales en la parte derecha de la ventana.



7. Seleccione una tarea local que desee ejecutar, detener, suspender o reanudar.

8. Realice la acción necesaria en la tarea mediante uno de los siguientes métodos:

- Haga clic con el botón derecho del ratón para abrir el menú contextual de la tarea local y seleccione **Ejecutar / Detener / Suspender / Reanudar**.
- Para iniciar o detener una tarea local, haga clic en el botón  /  situado a la derecha de la lista de tareas locales.
- Haga lo siguiente:
 - a. Haga clic en el botón **Propiedades** situado bajo la lista de tareas local o seleccione **Propiedades** en el menú contextual de la tarea.
Se abre la ventana **Propiedades: <Nombre de la tarea>**.
 - b. En la pestaña **General**, haga clic en el botón **Ejecutar / Detener / Suspender / Reanudar**.



Para iniciar, detener, suspender o reanudar una tarea de grupo:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, seleccione la carpeta que lleva el nombre del grupo de administración cuya tarea de grupo desee iniciar, detener, suspender o reanudar.
3. Seleccione la pestaña **Tareas** del espacio de trabajo.
Las tareas de grupo se muestran en la parte derecha de la ventana.
4. Seleccione una tarea de grupo que desee ejecutar, detener, suspender o reanudar.
5. Realice la acción necesaria en la tarea mediante uno de los siguientes métodos:

- En el menú contextual de la tarea de grupo, seleccione **Ejecutar / Detener / Suspender / Reanudar**.
- Haga clic en el botón  /  situado en la parte derecha de la ventana para iniciar o detener una tarea de grupo.

- Haga lo siguiente:
 - a. Haga clic en el enlace **Configuración de tareas** en la parte derecha del espacio de trabajo de la consola de administración o seleccione **Propiedades** en el menú contextual de la tarea.
Se abre la ventana **Propiedades: <Nombre de la tarea>**.
 - b. En la pestaña **General**, haga clic en el botón **Ejecutar / Detener / Suspender / Reanudar**.

Para iniciar, detener, suspender o reanudar una tarea para una selección de equipos, haga lo siguiente:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Tareas** del árbol de consola de administración, seleccione una tarea para la selección de equipos que desee ejecutar, detener, suspender o reanudar.
3. Realice una de las siguientes acciones:
 - En el menú contextual de la tarea, seleccione **Ejecutar / Detener / Suspender / Reanudar**.
 - Haga clic en el botón  /  situado en la parte derecha de la ventana a fin de iniciar o detener la tarea para equipos específicos.
 - Haga lo siguiente:
 - a. Haga clic en el enlace **Configuración de tareas** en la parte derecha del espacio de trabajo de la consola de administración o seleccione **Propiedades** en el menú contextual de la tarea.
Se abre la ventana **Propiedades: <Nombre de la tarea>**.
 - b. En la pestaña **General**, haga clic en el botón **Ejecutar / Detener / Suspender / Reanudar**.

Edición de la configuración de tareas

Para editar los parámetros de una tarea local, haga lo siguiente:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del [grupo de administración](#) al que pertenece el equipo cliente pertinente.
3. En el espacio de trabajo, seleccione la pestaña **Dispositivos**.
4. Seleccione un equipo para el cual desea configurar los ajustes de la aplicación.
5. Haga clic con el botón derecho del ratón para que aparezca el menú contextual del equipo cliente y seleccione **Propiedades**.
Se abre una ventana de propiedades del equipo cliente.
6. Seleccione la sección **Tareas**.
Aparece una lista de tareas locales en la parte derecha de la ventana.
7. Seleccione la tarea local necesaria en la lista de tareas locales.

8. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:

- En el menú contextual de la directiva, seleccione **Propiedades**.
- Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.

9. En la ventana **Propiedades: <nombre de tarea local>**, seleccione la sección **Configuración**.

10. Edite la configuración de la tarea local.

11. Para guardar los cambios, en la ventana **Propiedades: <nombre de tarea local>**, haga clic en **Aceptar**.

12. Para guardar los cambios, en la ventana **Propiedades: <Nombre del equipo>**, haga clic en **Aceptar**.

Para editar los parámetros de un grupo de tareas, haga lo siguiente:

1. Abra la consola de administración de Kaspersky Security Center.

2. En la carpeta **Dispositivos administrados**, abra la carpeta que lleva el nombre del grupo de administración pertinente.

3. Seleccione la pestaña **Tareas** del espacio de trabajo.

Las tareas de grupo se muestran en el espacio de trabajo de la Consola de la administración.

4. Seleccione la tarea de grupo pertinente.

5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:

- En el menú contextual de la directiva, seleccione **Propiedades**.
- Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.

6. En la ventana **Propiedades: <Nombre de la tarea de grupo>**, seleccione la sección de **Configuración**.

7. Edite la configuración de tareas de grupo.

8. Para guardar los cambios, en la ventana **Propiedades: <nombre de tarea de grupo>**, haga clic en **Aceptar**.

Con objeto de editar la configuración de una tarea para un grupo de equipos, haga lo siguiente:

1. Abra la consola de administración de Kaspersky Security Center.

2. En la carpeta **Tareas** del árbol de la consola de administración, seleccione una tarea para una selección de equipos cuya configuración desee editar.

3. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:

- En el menú contextual de la directiva, seleccione **Propiedades**.
- Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.

4. En la ventana **Propiedades: <nombre de la tarea para una selección de equipos>**, seleccione la sección **Configuración**.

5. Edite la configuración de la tarea para la selección de equipos.

6. Para guardar los cambios, en la ventana **Propiedades: <nombre de la tarea para una selección de equipos>**, haga clic en **Aceptar**.

Excepto la sección **Configuración**, todas las secciones de la ventana Propiedades de la tarea son idénticas a las que se usan en Kaspersky Security Center. Para obtener una descripción detallada de ellos, consulte la *Guía de administrador de Kaspersky Security Center*. La sección **Configuración** contiene la configuración específica de Kaspersky Endpoint Security 10 para Windows. Su contenido depende de la tarea seleccionada o del tipo de tarea.

Gestión de directivas

En esta sección, se trata la creación y configuración de las directivas para Kaspersky Endpoint Security. Para obtener información detallada sobre la gestión de Kaspersky Endpoint Security utilizando directivas de Kaspersky Security Center, consulte la *Guía de administrador de Kaspersky Security Center*.

Acerca de las directivas

Puede usar directivas para aplicar parámetros de Kaspersky Endpoint Security idénticos a todos los equipos cliente de un grupo de administración.

Puede cambiar localmente los valores de configuración especificados por una directiva para equipos particulares en un grupo de administración que utilice Kaspersky Endpoint Security. Puede cambiar localmente solo los ajustes cuya modificación no esté prohibida por la directiva.

La posibilidad de modificar parámetros de aplicaciones en un equipo cliente la determina el estado de bloqueo en el parámetro de una directiva:

- Si un parámetro aparece "bloqueado" (🔒), no puede editar su valor de forma local. El valor del ajuste especificado por la directiva se utiliza para todos los equipos del cliente dentro del grupo de administración.
- Cuando un ajuste está "desbloqueado" (🔓), puede editarlo de forma local. Se aplicarán parámetros configurados localmente en todos los equipos clientes de un grupo de administración. No se aplicarán parámetros configurados mediante directivas.

Después de aplicar la directiva por primera vez, la configuración de la aplicación local cambia de acuerdo con la configuración de las directivas.

Los derechos de acceso a la configuración de las directivas (lectura, escritura, ejecución) se especifican para cada usuario que tenga acceso al servidor de administración de Kaspersky Security Center y, por separado, para cada cobertura funcional de Kaspersky Endpoint Security. Para configurar los derechos de acceso a la configuración de las directivas, vaya a la sección **Seguridad** de la ventana de propiedades del servidor de administración de Kaspersky Security Center.

Se seleccionan las siguientes coberturas funcionales de Kaspersky Endpoint Security:

- Protección antivirus. La cobertura funcional incluye Antivirus de archivos, Antivirus del correo, Antivirus Internet, Antivirus para chat, Análisis de vulnerabilidades y Tareas de análisis.
- Control de inicio de aplicaciones. La cobertura funcional incluye el componente Control de inicio de aplicaciones.

- Control de dispositivos. La cobertura funcional incluye el componente Control de dispositivos.
- Cifrado. La cobertura funcional incluye el disco duro, el archivo y los componentes de cifrado de carpetas.
- Zona de confianza. La cobertura funcional incluye la zona de confianza.
- Control web. La cobertura funcional incluye el componente Control Web.
- Prevención de intrusiones. Esta cobertura funcional incluye los componentes Supervisión de la actividad de aplicaciones, Control de vulnerabilidades, Firewall, Prevención de intrusiones y Control de actividad de aplicaciones.
- Funcionalidad básica. Esta cobertura funcional incluye ajustes generales de la aplicación no especificados para otras coberturas funcionales como los siguientes: licencias, configuración de KSN, tareas del inventario, tareas de actualización de módulos y bases de datos de la aplicación, autoprotección, configuración avanzada de la aplicación, informes y almacenes, configuración de la protección con contraseña, y configuración de la interfaz de la aplicación.

Puede realizar las siguientes operaciones de directiva:

- Crear una directiva.
- Modificar parámetros de directivas.

Si la cuenta de usuario con la que accedió al servidor de administración no tiene derechos para modificar la configuración de ciertas coberturas funcionales, no es posible modificar la configuración de dichas coberturas funcionales.

- Eliminar una directiva.
- Cambiar el estado de una directiva.

Consulte la *Guía de administrador de Kaspersky Security Center* para obtener información sobre el uso de directivas que no están relacionadas con la interacción con Kaspersky Endpoint Security.

Creación de una directiva

Para crear una directiva, haga lo siguiente:

1. Abra la consola de administración de Kaspersky Security Center.
2. Realice una de las siguientes acciones:
 - Seleccione la carpeta **Dispositivos administrados** del árbol de la consola de administración a fin de crear una directiva para todos los equipos que administra Kaspersky Security Center.
 - En la carpeta **Dispositivos administrados** del árbol de la consola de administración, seleccione la carpeta que lleva el nombre del grupo de administración al que pertenecen los equipos cliente pertinentes.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Realice una de las siguientes acciones:

- Haga clic en el botón **Crear directiva**.
- Haga clic con el botón derecho del ratón para abrir el menú contextual y seleccione **Crear Directiva**.

El Asistente de directivas se inicia.

5. Siga las instrucciones del Asistente de directivas.

Edición de la configuración de directivas

Para modificar valores de directiva:

1. Abra la consola de administración de Kaspersky Security Center.
2. En la carpeta **Dispositivos administrados** del árbol de la consola de administración, abra la carpeta que lleva el nombre del grupo de administración pertinente para el que desea editar la configuración de directivas.
3. En el espacio de trabajo, seleccione la pestaña **Directivas**.
4. Seleccione la directiva necesaria.
5. Abra la ventana **Propiedades: <Nombre de directiva>** usando uno de los siguientes métodos:
 - En el menú contextual de la directiva, seleccione **Propiedades**.
 - Haga clic en el enlace **Configurar directiva** situado en la parte derecha del espacio de trabajo de la consola de administración.

La configuración de la directiva de Kaspersky Endpoint Security 10 para Windows incluye la configuración de las tareas y la [configuración de la aplicación](#). Las secciones **Protección antivirus** y **Control de Endpoint** de la ventana **Propiedades: <Nombre de directiva>** muestra los ajustes de los componentes de protección y control, la sección **Cifrado de datos** muestra los ajustes de cifrado para archivos y carpetas, y la sección **Configuración avanzada** muestra la configuración de la aplicación.

Para activar la visualización de la configuración del cifrado de datos y de los componentes de control en la configuración de la directiva, debe seleccionar las casillas de verificación correspondientes en la ventana **Configuración de la interfaz** de Kaspersky Security Center.

6. Modifique la configuración de directivas.
7. Para guardar los cambios, en la ventana **Propiedades: <Nombre de directiva>**, haga clic en **Aceptar**.

Selección de los ajustes que se mostrarán en la política de Kaspersky Security Center

Para seleccionar la configuración que se mostrará en la directiva de Kaspersky Security Center:

1. Abra la consola de administración de Kaspersky Security Center.
2. En el menú contextual del nodo **Servidor de administración - <nombre del equipo>** del árbol de la consola de administración, seleccione Ver → **Configuración de la interfaz**.

Se abre la ventana **Configuración de la interfaz**.

3. En la ventana **Configuración de la interfaz**, seleccione las casillas de verificación situadas junto a la configuración que se debe mostrar en la configuración de creación de directivas de Kaspersky Security Center y en las propiedades de la directiva:
 - Seleccione la casilla de verificación **Mostrar componentes de control de endpoint** para activar la visualización de la configuración de los componentes de control en la ventana del Asistente de directivas de Kaspersky Security Center y en las propiedades de la directiva.
 - Seleccione la casilla de verificación **Mostrar cifrado y protección de datos** para activar la visualización de la configuración del cifrado de datos en la ventana del Asistente de nueva directiva de Kaspersky Security Center y en las propiedades de la directiva.
4. Haga clic en **Aceptar**.

Enviar mensajes del usuario al servidor de Kaspersky Security Center

Es posible que un usuario deba enviar un mensaje al administrador de la red corporativa local en los casos siguientes:

- Control de dispositivos bloqueó el acceso al dispositivo.
La plantilla del mensaje para una solicitud de acceso a un dispositivo bloqueado está disponible en la interfaz de Kaspersky Endpoint Security, en la sección [Control de dispositivos](#).
- Control de inicio de aplicaciones bloqueó el inicio de una aplicación.
La plantilla del mensaje para solicitar permiso para el inicio de una aplicación bloqueada está disponible en la interfaz de Kaspersky Endpoint Security en la sección [Control de Inicio de Aplicaciones](#).
- Control Web bloqueó el acceso a un recurso web.
La plantilla del mensaje para solicitar acceso a un recurso web bloqueado está disponible en la interfaz de Kaspersky Endpoint Security, en la sección [Control Web](#).

El método usado para enviar mensajes y la plantilla utilizada dependen de si hay una directiva activa de Kaspersky Security Center que se ejecuta en el equipo que tiene Kaspersky Endpoint Security instalado, y si hay alguna conexión con el servidor de administración de Kaspersky Security Center. Son posibles las siguientes situaciones:

- Si una directiva de Kaspersky Security Center no se está ejecutando en el equipo donde se ha instalado Kaspersky Security Center, el mensaje del usuario se envía al administrador de la red de área local por correo electrónico.
Los campos del mensaje se rellenan con los valores de los campos de la plantilla definida en la interfaz local de Kaspersky Endpoint Security.
- Si una directiva de Kaspersky Security Center se está ejecutando en el equipo donde se ha instalado Kaspersky Security Center, el mensaje estándar se envía al servidor de administración de Kaspersky Security Center.
En este caso, los mensajes del usuario están disponibles para su visualización en el [almacén de eventos de Kaspersky Security Center](#). Los campos del mensaje se rellenan con los valores de los campos de la plantilla definida en la directiva de Kaspersky Security Center.
- Si la directiva para casos en los que el equipo está fuera de la oficina de Kaspersky Security Center está ejecutándose en el equipo donde se ha instalado Kaspersky Endpoint Security, el método usado para enviar mensajes depende de si existe una conexión con Kaspersky Security Center.

- Si se establece una conexión con Kaspersky Security Center, Kaspersky Endpoint Security envía el mensaje estándar al servidor de administración de Kaspersky Security Center.
- Si falta una conexión con Kaspersky Security Center, el mensaje del usuario se envía al administrador de la red de área local por correo electrónico.

En ambos casos, los campos del mensaje se rellenan con los valores de los campos de la plantilla definida en la directiva de Kaspersky Security Center.

Visualización de los mensajes del usuario en el almacén de eventos de Kaspersky Security Center

Los componentes [Control de inicio de aplicaciones](#), [Control de dispositivos](#) y [Control Web](#) permiten que los usuarios de la red de área local que dispongan de equipos con Kaspersky Endpoint Security envíen mensajes al administrador.

Un usuario puede enviar mensajes al administrador mediante dos métodos:

- Como un evento en el almacén de eventos de Kaspersky Security Center.
Se envía un mensaje con el evento de usuario al almacén de eventos de Kaspersky Security Center si la aplicación de Kaspersky Endpoint Security instalada en el equipo del usuario funciona de acuerdo con la directiva activa.
- Como un mensaje de correo electrónico.
La información del usuario se envía por correo electrónico si la aplicación Kaspersky Endpoint Security que se instala en el equipo del usuario no está ejecutando una directiva o bien está ejecutando una directiva para casos en los que el equipo está fuera de la oficina.

Para ver el mensaje de un usuario en el almacén de eventos de Kaspersky Security Center:

1. Abra la consola de administración de Kaspersky Security Center.
2. En el nodo **Servidor de administración** del árbol de la consola de administración, seleccione la pestaña **Eventos**.
El espacio de trabajo de Kaspersky Security Center muestra todos los eventos que se producen durante el funcionamiento de Kaspersky Endpoint Security, incluidos los mensajes al administrador que se reciben de los usuarios de la red de área local.
3. Para configurar el filtro del evento, en la lista desplegable **Seleccionar eventos**, seleccione **Solicitudes de usuario**.
4. Seleccione el mensaje que se enviará al administrador.
5. Abra la ventana **Propiedades del evento** de una de estas formas:
 - Haga clic con el botón derecho del ratón en el evento. En el menú contextual que se abre, seleccione **Propiedades**.
 - Haga clic en el botón **Abrir la ventana de propiedades del evento** en la parte derecha del espacio de trabajo de la consola de administración.

Participación en Kaspersky Security Network

Esta sección contiene información sobre la participación en Kaspersky Security Network e instrucciones sobre cómo activar o desactivar el uso de Kaspersky Security Network.

Acerca de la participación en Kaspersky Security Network

Para proteger su equipo de manera más efectiva, Kaspersky Endpoint Security utiliza los datos recopilados de los usuarios de todo el mundo. *Kaspersky Security Network* está diseñada para recopilar dichos datos.

Kaspersky Security Network (KSN) es una infraestructura de servicios en la nube que brinda acceso a la Base de conocimientos de Kaspersky, un recurso en línea que permite conocer la reputación de los archivos, los recursos web y el software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas por parte de Kaspersky Endpoint Security ante nuevas amenazas, mejora el rendimiento de algunos componentes de protección y reduce el riesgo probable de que se produzcan falsos positivos.

Según la ubicación de la infraestructura, hay un servicio KSN global (los servidores de Kaspersky alojan la infraestructura) y un servicio KSN local (los servidores de terceros alojan la infraestructura, por ejemplo, en la red del proveedor de servicios de Internet).

Tras cambiar la licencia, envíe los detalles de la nueva clave al proveedor de servicios para poder utilizar KSN privada. De lo contrario, el intercambio de datos con KSN no será posible.

Gracias a quienes participan en KSN, Kaspersky puede recibir rápidamente información sobre los distintos tipos de amenazas y sus orígenes, desarrollar soluciones para neutralizar estos riesgos y reducir la cantidad de falsas alarmas que muestran los componentes de la aplicación.

Al participar en KSN, la aplicación envía automáticamente estadísticas generadas a KSN mientras se ejecuta la aplicación. La aplicación también puede enviar determinados archivos (o partes de los archivos) que los hackers podrían utilizar para dañar el equipo, o bien datos a Kaspersky para un análisis adicional.

No se recopilan, procesan ni almacenan datos personales. La Declaración de Kaspersky Security Network y el [sitio web de Kaspersky](#) contienen más detalles sobre la información que se genera cuando el usuario participa en KSN, sobre la transmisión de dicha información a Kaspersky y sobre el almacenamiento y la destrucción de dicha información. El archivo ksn_<ID de idioma>.txt con el texto de la declaración de Kaspersky Security Network se incluye en el kit de distribución de la aplicación.

Para reducir la carga en los servidores de KSN, Kaspersky puede lanzar bases de datos antivirus de la aplicación que desactivan temporalmente o restringen en parte las solicitudes a Kaspersky Security Network. En este caso, el [estado de la conexión a KSN](#) aparece como [Activado con restricciones](#).

Los equipos de los usuarios que gestionen el servidor de administración de Kaspersky Security Center pueden interactuar con KSN mediante el servicio de proxy de KSN.

El servicio de proxy de KSN ofrece las siguientes funcionalidades:

- El equipo del usuario puede consultar y enviar información a KSN, aunque no tenga acceso directo a Internet.

- Proxy de KSN almacena en caché los datos procesados, por lo que reduce la carga de la conexión de red externa y acelera la recepción de la información que necesita el usuario del equipo.

Puede obtener más detalles sobre el servicio de proxy de KSN en la *Guía de administrador de Kaspersky Security Center*.

Se puede ajustar la configuración del proxy de KSN en las propiedades de la directiva de [Kaspersky Security Center](#).

La participación en Kaspersky Security Network es voluntaria. La aplicación invita al usuario a participar en KSN durante la configuración inicial de la aplicación. Los usuarios podrán reanudar o interrumpir su participación en KSN en cualquier momento.

Activación y desactivación del uso de Kaspersky Security Network

Para activar o desactivar el uso de Kaspersky Security Network:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, en la sección **Configuración avanzada**, seleccione el apartado **Configuración de KSN**.

La configuración de Kaspersky Security Network se muestra en la parte derecha de la ventana.

3. Realice una de las siguientes acciones:

- Para activar el uso de Kaspersky Security Network, seleccione la casilla de verificación **Acepto la declaración de KSN y las condiciones de participación**.
- Para desactivar el uso de Kaspersky Security Network, desactive la casilla de verificación **Acepto la declaración de KSN y las condiciones de participación**.

4. Para guardar los cambios realizados, haga clic en el botón **Guardar**.

Comprobación de la conexión a Kaspersky Security Network

Para comprobar la conexión a Kaspersky Security Network:

1. Abra la [ventana principal de la aplicación](#).
2. En la parte superior de la ventana, haga clic en el botón **Kaspersky Security Network**.

Se abre la ventana **Kaspersky Security Network**.

La parte izquierda de la ventana **Kaspersky Security Network** muestra el modo de conexión a Kaspersky Security Network con forma de botón de **KSN** redondo:

- Si Kaspersky Endpoint Security no está conectado a Kaspersky Security Network, el color del botón de **KSN** es gris. En el estado que aparece debajo del botón **KSN**, se lee *Desactivado*.
- Si Kaspersky Endpoint Security está conectado a Kaspersky Security Network y los servidores de KSN están disponibles, el botón **KSN** aparece de color verde. La siguiente información aparece bajo el botón **KSN**: estado *Activado*, tipo de KSN en uso (**KSN privada** o **KSN global**) y la fecha y hora de la última sincronización con los servidores KSN. La parte derecha de la ventana muestra estadísticas sobre la reputación de los archivos, los recursos web y el software.

Kaspersky Endpoint Security recopila datos estadísticos sobre el uso de KSN cuando abre la ventana **Kaspersky Security Network**. Las estadísticas no están actualizadas en tiempo real.

- Si Kaspersky Endpoint Security está conectado a Kaspersky Security Network, pero los servidores de KSN no están disponibles, el botón **KSN** aparece de color rojo. En el estado que aparece debajo del botón **KSN**, se lee *Activado*.

Si la hora de la última sincronización con los servidores KSN supera los 15 minutos o presenta el estado *Desconocido*, esto significa que los servidores KSN no están disponibles. En tal caso, le recomendamos que se ponga en contacto con el Soporte técnico o su proveedor de servicios.

Puede que no exista conexión a los servidores de Kaspersky Security Network por los siguientes motivos:

- El equipo no está conectado a Internet.
- La aplicación no se ha activado o la licencia ha caducado.
- Se han detectado problemas relacionados con la clave (por ejemplo, la clave se ha incluido en la lista negra).

Comprobar la reputación de un archivo en Kaspersky Security Network

El servicio de KSN le permite recuperar la información sobre las aplicaciones incluidas en las bases de datos de reputación de Kaspersky. Esto activa la administración flexible de directivas de inicio de aplicaciones a nivel de la empresa, lo cual evita el inicio de software publicitario y otros programas que pueden utilizar los criminales para dañar su equipo o sus datos personales.

Para comprobar la reputación de un archivo en Kaspersky Security Network:

1. Haga clic con el botón derecho del ratón para acceder al menú contextual del archivo cuya reputación desea comprobar.
2. Seleccione la opción **Comprobar reputación en KSN**.

Esta opción está disponible si ha aceptado los términos de la [Declaración de Kaspersky Security Network](#).

Esto abre la ventana **<nombre del archivo> - Reputación en KSN**. La ventana **<nombre de archivo> - la Reputación en KSN** muestra información siguiente sobre el archivo comprobado:

- **Ruta.** Ruta en la que el archivo se guarda en el disco.
- **Versión.** Versión de la aplicación (la información solo se muestra para los archivos ejecutables).
- **Firma digital.** Presencia de una firma digital con el archivo.
- **Firmado.** La fecha en la cual el certificado se firmó con una firma digital.
- **Creado.** Fecha de creación del archivo.

- **Modificado.** Fecha de la última modificación del archivo.
- **Tamaño.** Espacio en disco ocupado por el archivo.
- Información sobre el número de usuarios confían en el archivo o lo bloquean.

Protección mejorada con Kaspersky Security Network

Kaspersky ofrece una capa adicional de protección a los usuarios mediante Kaspersky Security Network. Este método de protección está diseñado para combatir amenazas avanzadas persistentes y ataques de día cero. Las tecnologías en la nube integradas y la experiencia de los analistas antivirus de Kaspersky hacen de Kaspersky Endpoint Security una opción inigualable para la protección contra las amenazas de red más sofisticadas.

Los detalles acerca de la protección mejorada de Kaspersky Endpoint Security están disponibles en el sitio web de Kaspersky.

Fuentes de información de la aplicación

La página de Kaspersky Endpoint Security del sitio web de Kaspersky

En [la página de Kaspersky Endpoint Security](#), encontrará información general sobre la aplicación, sus características y sus funciones.

La página de Kaspersky Endpoint Security contiene un enlace a la tienda en línea. Desde ella, podrá comprar o renovar la aplicación.

La página de Kaspersky Endpoint Security en la Base de conocimientos

La *Base de conocimientos* es una sección del sitio web del Soporte técnico.

En [la página de Kaspersky Endpoint Security en la Base de conocimientos](#) puede leer artículos que ofrecen información, recomendaciones y respuestas útiles a preguntas frecuentes sobre cómo adquirir, instalar y utilizar la aplicación.

Los artículos de la Base de conocimientos pueden contestar preguntas que se relacionan no solo con Kaspersky Endpoint Security, sino también con otras aplicaciones de Kaspersky. Los artículos también pueden contener novedades del Servicio de soporte técnico.

Discusiones sobre las aplicaciones de Kaspersky en el foro

Si su pregunta no requiere una respuesta urgente, puede compartirla con los expertos de Kaspersky y con otros usuarios en nuestro [Foro](#).

En este foro puede ver los temas existentes, dejar sus comentarios y crear nuevos temas de debate.

Cómo ponerse en contacto con el Soporte técnico

Esta sección describe las formas en que se puede recibir asistencia del soporte técnico y las condiciones en que está disponible.

Cómo obtener soporte técnico

Si no es posible encontrar una solución al problema en la documentación de la aplicación o en uno de los [orígenes de información acerca de la aplicación](#), le recomendamos que se ponga en contacto con Soporte técnico. Los especialistas de Soporte técnico responderán a sus preguntas sobre la instalación y uso de la aplicación.

El soporte técnico solo está disponible para aquellos usuarios que han adquirido una licencia comercial. Los usuarios que hayan recibido una licencia de evaluación no podrán acceder al soporte técnico.

Antes de ponerse en contacto con el Soporte técnico, lea las [reglas de soporte](#).

Puede ponerse en contacto con Soporte técnico de una de las siguientes formas:

- [Llamando por teléfono al Soporte técnico](#)
- Enviando una solicitud al Soporte técnico de Kaspersky a través del [portal CompanyAccount de Kaspersky](#)

Soporte técnico por teléfono

Puede llamar por teléfono a representantes del Soporte técnico de la mayoría de las regiones del mundo. Puede obtener información sobre las formas de recibir el soporte técnico en su región y los contactos de Soporte Técnico en el [sitio web de Soporte Técnico de Kaspersky](#).

Antes de ponerse en contacto con el Soporte técnico, lea las [reglas de soporte](#).

Soporte técnico a través de CompanyAccount de Kaspersky

[Kaspersky CompanyAccount](#) es un portal para empresas que utilizan aplicaciones de Kaspersky. El portal CompanyAccount de Kaspersky se ha diseñado para facilitar la interacción entre los usuarios y los expertos de Kaspersky a través de solicitudes electrónicas. Puede usar el portal CompanyAccount de Kaspersky para realizar el seguimiento del estado de sus solicitudes electrónicas y guardar el historial de dichas solicitudes.

Puede registrar a todos los empleados de su organización bajo una única cuenta en CompanyAccount de Kaspersky. Dicha cuenta única le permitirá gestionar de forma centralizada las solicitudes electrónicas de los empleados registrados en Kaspersky y, asimismo, gestionar los privilegios de dichos empleados a través de CompanyAccount de Kaspersky.

El portal CompanyAccount de Kaspersky 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 Soporte Técnico](#).

Recopilación de información para el Soporte técnico

Después de informar a los especialistas de Soporte técnico de Kaspersky acerca del problema, puede que le pidan que cree un *archivo de seguimiento*. El archivo de seguimiento permite supervisar poco a poco el proceso de ejecución de comandos de aplicación y determinar la etapa de funcionamiento de la aplicación en la que se produce el error.

Los especialistas de Soporte técnico pueden solicitar también información adicional sobre el sistema operativo, los procesos en ejecución del equipo, los informes detallados sobre el funcionamiento de los componentes de aplicación y los volcados de memoria de la aplicación.

Puede recopilar la información necesaria con la ayuda de Kaspersky Endpoint Security. La información recopilada se puede guardar en el disco duro y cargarla más adelante, cuando le resulte más cómodo.

Mientras el diagnóstico está en ejecución, los expertos del Soporte técnico pueden pedir que cambie la configuración de la aplicación por:

- Activar la funcionalidad que recopila la información de diagnóstico extendido.
- Ajustar la configuración de los componentes individuales de la aplicación, que no están disponibles a través de los elementos estándar de la interfaz de usuario.
- Cambiar la configuración del almacenamiento y de la transmisión de la información de diagnóstico recopilada.
- Configurar la interceptación y el registro del tráfico de red.


Los expertos de Soporte técnico le proporcionarán toda la información necesaria para realizar dichas operaciones (descripción de la secuencia de pasos, ajustes que se deben modificar, archivos de configuración, scripts, funcionalidad adicional de la línea de comandos, módulos de depuración, utilidades especiales, etc.) y le informarán acerca del alcance de los datos recopilados para la depuración. La información de diagnóstico extendido que se recopile se guarda en el equipo del usuario. Los datos recopilados no se transmiten a Kaspersky automáticamente.

Los ajustes utilizados para determinar la dirección del servidor de volcado con el fin de enviar archivos de volcado a Kaspersky se guardan en el equipo del usuario. Si es necesario, los valores de estos ajustes se pueden editar en la clave de registro del sistema operativo "DumpServerConfigUrl"="https://dmconfig.kaspersky-labs.com/dumpserver/config.xml".

Las operaciones que se describen anteriormente solo se deben realizar bajo la supervisión de los especialistas de Soporte técnico siguiendo sus instrucciones. Los cambios no supervisados que se realicen a la configuración de la aplicación de forma distinta a la que se describe en la Guía del administrador o a las instrucciones de los especialistas de Soporte técnico pueden ralentizar o bloquear el sistema operativo, afectar a seguridad del equipo o poner en peligro la disponibilidad y la integridad de los datos que se estén procesando.

Creación de un archivo de depuración

Para crear un archivo de seguimiento:

1. Abra la [ventana principal de la aplicación](#).
2. En la ventana de la aplicación principal, haga clic en el botón .
Se abre la ventana **Soporte**.
3. En la ventana **Soporte**, haga clic en el botón **Rastreo del sistema**.
Se abre la ventana **Información para el Soporte técnico**.
4. Para iniciar el proceso de rastreo, active la casilla de verificación **Activar rastreo**.
5. En la lista desplegable **Nivel**, seleccione el nivel de seguimiento.
Se le aconseja que aclare el nivel de seguimiento necesario con un especialista de Soporte técnico. Si no dispone de asistencia por parte del Soporte técnico, establezca el nivel de seguimiento en **Normal (500)**.
6. Reproduzca la situación en la que se produjo el problema.
7. Para detener el proceso de rastreo, vuelva a **Información para el Soporte Técnico** y desactive la casilla de verificación **Activar rastreo**.

Después de crear el archivo de seguimiento, puede [cargar los resultados del seguimiento en el servidor de Kaspersky](#).

Contenido y almacenamiento de archivos de seguimiento

El usuario es personalmente responsable de garantizar la seguridad de los datos recopilados y, especialmente, de supervisar y restringir el acceso a los datos recopilados almacenados en el equipo hasta que se envíe a Kaspersky.

Los archivos de rastreo se almacenan en el equipo en formato modificado que no puede leerse siempre que la aplicación esté en uso y se eliminan permanentemente cuando se quita la aplicación.

Los archivos de seguimiento se almacenan en la carpeta ProgramData\Kaspersky Lab.

El archivo de seguimiento tiene el siguiente formato de nombre: KES<número de versión_fechaXX.XX_horaXX.XX_pidXXX.><tipo de archivo de seguimiento>.log.enc1.

El archivo de rastreo del Agente de autenticación se almacena en la carpeta Información del volumen del sistema y tiene el nombre siguiente: KLFDE . {EB2A5993-DFC8-41a1-B050-F0824113A33A} .PBELOG .bin.

Puede ver los datos almacenados en los archivos de seguimiento. Póngase en contacto con el Soporte Técnico de Kaspersky para recibir indicaciones de cómo ver los datos.

Todos los archivos de seguimiento contienen los datos comunes siguientes:

- Hora del evento.
- Número del subprocesso de ejecución.

El archivo de rastreo del Agente de autenticación no contiene esta información.

- Componente de la aplicación que causó el evento.
- Nivel de gravedad de eventos (evento informativo, advertencia, evento crítico, error).
- Una descripción del evento que implica la ejecución del comando por un componente de la aplicación y el resultado de la ejecución de este comando.

Contenidos de los archivos de seguimiento SRV.log, GUI.log y ALL.log

Los archivos de seguimiento SRV.log, GUI.log y ALL.log pueden almacenar la siguiente información además de datos generales:

- Datos personales, incluido el apellido, el nombre y el segundo nombre, si se incluyen estos datos en la ruta a los archivos en un equipo local.
- El nombre de usuario y la contraseña si se transmitieron abiertamente. Estos datos se pueden registrar en archivos de seguimiento durante el análisis del tráfico de Internet. El tráfico se registra en archivos de seguimiento solo desde trafmon2.ppl.
- El nombre de usuario y la contraseña si se incluyen en encabezados HTTP.
- El nombre de la cuenta de Microsoft Windows si se incluye el nombre de la cuenta en un nombre de archivo.
- Su dirección de correo electrónico o una dirección web que contenga el nombre y la contraseña de su cuenta si se incluyen en el nombre del objeto detectado.
- Los sitios web que visita y a los que se le redirige desde estos. Estos datos se escriben en archivos de seguimiento cuando la aplicación analiza sitios web.
- Dirección del servidor proxy, nombre del equipo, puerto, dirección IP y nombre de usuario usado para iniciar sesión en el servidor proxy. Estos datos se escriben en los archivos de seguimiento si la aplicación utiliza a un servidor proxy.
- Direcciones IP remotas con las que el equipo establece conexiones.
- Asunto del mensaje, ID, nombre y dirección del remitente de la página web del remitente del mensaje en una red social. Estos datos se escriben en archivos de rastreo si el componente Control web está activado.

Contenido de los archivos de seguimiento HST.log, BL.log, Dumpwriter.log, WD.log y AVPCon.dll.log

Además de datos generales, el archivo de rastreo HST.log contiene información sobre la ejecución de una tarea de la actualización de la base de datos y del módulo de aplicación.

Además de datos generales, el archivo de seguimiento BL.log contiene información sobre los eventos que ocurren durante el funcionamiento de la aplicación, así como los datos requeridos para solucionar problemas de errores de aplicación. Este archivo se crea si se inicia la aplicación con el parámetro -bl de avp.exe.

Además de datos generales, el archivo de rastreo Dumpwriter.log contiene información de servicio requerida para solucionar errores que se producen cuando se escribe el archivo de volcado de la aplicación.

Además de datos generales, el archivo de rastreo WD.log contiene información sobre los eventos que se producen durante el funcionamiento del servicio avpsus, incluidos eventos de actualización del módulo de aplicación.

Además de datos generales, el archivo de seguimiento AVPCon.dll.log contiene información sobre los eventos que se producen durante el funcionamiento del módulo de conectividad de Kaspersky Security Center.

Contenido de archivos de seguimiento de los complementos de la aplicación

Los archivos de seguimiento de los complementos de la aplicación contienen la información siguiente además de datos generales:

- El archivo de seguimiento shellex.dll.log del complemento que inicia la tarea de análisis en el menú contextual contiene información sobre la ejecución de la tarea de análisis y los datos requeridos para depurar el complemento.
- El archivo de seguimiento mcou.OUTLOOK.EXE del complemento Antivirus del correo puede contener partes de mensajes de correo electrónico, incluidas direcciones de correo electrónico.

Contenidos del archivo de rastreo del Agente de autenticación

Además de datos generales, el archivo de rastreo del Agente de autenticación contiene información sobre el funcionamiento del Agente de autenticación y las acciones que el usuario lleva a cabo con el Agente de autenticación.

Activar o desactivar el envío de archivos de volcado y rastreo a Kaspersky

Para activar o desactivar la transmisión de archivos de volcado y rastreo a Kaspersky:

1. Abra la [ventana de configuración de la aplicación](#).
2. En la parte izquierda de la ventana, seleccione la sección **Configuración avanzada**.
La configuración avanzada de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Modo de funcionamiento**, haga clic en el botón **Configuración**.
Se abre la ventana **Modo de funcionamiento**.
4. En la ventana **Modo de funcionamiento**, seleccione la casilla de verificación **Activar escritura de volcado** para permitir que la aplicación escriba archivos de volcado de la aplicación.

5. Realice una de las siguientes acciones:

- Seleccione la casilla de verificación **Enviar archivos de volcado y de trazas a Kaspersky** si desea que la aplicación muestre una solicitud en la ventana **Transferencia al servidor de los datos para el Soporte Técnico** para enviar los archivos de volcado y rastreo a Kaspersky para el análisis de las causas del bloqueo de la aplicación en el siguiente inicio que se haga de esta.
- Si no, desactive la casilla de verificación **Enviar archivos de volcado y de trazas a Kaspersky**.

6. Haga clic en **Aceptar** en la ventana **Modo de funcionamiento**.

7. Para guardar los cambios, haga clic en el botón **Guardar** en la ventana principal de la aplicación.

Enviar archivos al servidor de Soporte técnico

Los archivos que contienen información sobre el sistema operativo, los archivos de rastreo y los archivos de volcado se deben enviar a expertos del Soporte Técnico de Kaspersky.

Para enviar archivos de datos al servidor de Soporte técnico:

1. Reinicie Kaspersky Endpoint Security tras un mal funcionamiento.

Esto abre la ventana **Error al iniciar la aplicación anterior**.

La ventana **Error al iniciar la aplicación anterior** se abrirá cada vez que Kaspersky Endpoint Security se inicie (lo que incluye después de reiniciar el equipo) hasta que envíe los archivos de volcado y rastreo a Soporte técnico o hasta que haga clic en el botón **No enviar**.

2. En la ventana **Error al iniciar la aplicación anterior**, abra la lista de archivos generados haciendo clic **aquí**.

3. Seleccione las casillas de verificación que hay junto a esos archivos que desea enviar al Soporte técnico.

4. Haga clic en el botón **Mostrar texto de la declaración**.

Se abre la ventana **Declaración de provisión de datos**.

5. Lea el texto de la Declaración de provisión de datos y haga clic en el botón **Cerrar**.

6. En la ventana **Error al iniciar la aplicación anterior**, seleccione **Acepto la declaración de provisión de datos**.

7. Haga clic en el botón **Enviar**.

Esto abre la ventana **Número de solicitud**.

8. En la ventana **Número de solicitud**, especifique el número que se asignó a su solicitud al ponerse en contacto con Soporte técnico mediante Kaspersky CompanyAccount.

9. Haga clic en **Aceptar**.

Los archivos de datos seleccionados se comprimen y se envían al servidor de Soporte técnico.

Habilitar y deshabilitar la protección de archivos de volcado y archivos de rastreo

Los archivos de volcado y rastreo contienen información sobre el sistema operativo, así como [datos confidenciales del usuario](#). Para evitar el acceso no autorizado a dichos datos, puede activar la protección de los archivos de volcado y rastreo.

Si se activa la protección de los archivos de volcado y rastreo, los usuarios siguientes pueden acceder a dichos archivos:

- El administrador del sistema y el administrador local pueden acceder a los archivos de volcado, así como el usuario que activó la escritura de los archivos de volcado y rastreo.
- Únicamente el administrador del sistema y el administrador del equipo local pueden acceder a los archivos de rastreo.

Para activar o desactivar la protección de los archivos de volcado y rastreo:

1. Abra la [ventana de configuración de la aplicación](#).
2. Seleccione la sección **Configuración avanzada** a la izquierda.
La configuración de la aplicación se muestra en la parte derecha de la ventana.
3. En la sección **Modo de funcionamiento**, haga clic en el botón **Configuración**.
Se abre la ventana **Modo de funcionamiento**.
4. Realice una de las siguientes acciones:
 - Seleccione la casilla de verificación **Activar la protección de los archivos de volcado y de trazas** si desea activar la protección.
 - Desactive la casilla de verificación **Activar la protección de los archivos de volcado y de trazas** si desea desactivar la protección.
5. Haga clic en **Aceptar** en la ventana **Modo de funcionamiento**.
6. Para guardar los cambios, haga clic en el botón **Guardar** en la ventana principal de la aplicación.

Los archivos de volcado y rastreo que se escribieron mientras la protección estaba activa permanecen protegidos incluso después de que esta función se desactive.

Glosario

Actualización

El procedimiento de reemplazo o adición de archivos nuevos (bases de datos o módulos de aplicación) que se han recuperado de los servidores de actualizaciones de Kaspersky.

Administrador de archivos portátiles

Este es una aplicación que proporciona una interfaz para trabajar con archivos cifrados en discos extraíbles cuando no hay ninguna funcionalidad de cifrado disponible en el equipo.

Agente de autenticación

Interfaz que permite autenticarse para acceder a discos duros cifrados y cargar el sistema operativo después del cifrado del disco duro del sistema.

Agente de red

Un componente de Kaspersky Security Center que permite la interacción entre el servidor de administración y las aplicaciones de Kaspersky instaladas en un nodo de red específico (estación de trabajo o servidor). Este componente es común a todas las aplicaciones de Kaspersky que se ejecutan con Windows. Las versiones dedicadas del Agente de red están destinadas para aplicaciones que se ejecutan con otros sistemas operativos.

Análisis de firmas

Tecnología de detección de amenazas que utiliza las bases de datos de Kaspersky Endpoint Security y contiene descripciones de amenazas conocidas y métodos para erradicarlas. La protección que utiliza el análisis de firmas proporciona un nivel de seguridad mínimo aceptable. Si se siguen las recomendaciones de los expertos de Kaspersky, este método está siempre activado.

Análisis heurístico

La tecnología se ha desarrollado para encontrar amenazas que no pueden detectarse con la versión actual de las bases de datos de la aplicación Kaspersky. Detecta archivos que pueden estar infectados con un virus desconocido o con una nueva variedad de virus conocidos.

Archivador

Uno o varios archivos comprimidos en un solo archivo comprimido. Se requiere una aplicación especializada llamada "archivador" para comprimir y descomprimir datos.

Archivo infectable

Un archivo que, por su estructura o formato, puede ser utilizado por intrusos como "contenedor" y distribuidor de un código malicioso. Como regla, estos son archivos ejecutables, con extensiones de archivo como .com, .exe y .dll. Existe un riesgo realmente elevado de intrusión de código malicioso en estos archivos.

Archivo infectado

Un archivo que contiene código malicioso (se ha detectado código de software malicioso [malware] conocida durante el análisis del archivo). Kaspersky no recomienda utilizar estos archivos, ya que podrían infectar el equipo.

Archivo probablemente infectado

Un archivo que contiene código modificado de un virus conocido o código que se parece al de un virus, pero que Kaspersky todavía no conoce. El Analizador heurístico detecta archivos probablemente infectados.

Base de datos de direcciones web fraudulentas

Una lista de direcciones web que los especialistas de Kaspersky han determinado como fraudulentas. La base de datos se actualiza con regularidad y forma parte del kit de distribución de la aplicación de Kaspersky.

Base de datos de direcciones web maliciosas

Lista de direcciones web cuyo contenido puede considerarse como peligroso. Los especialistas de Kaspersky se encargan de crear la lista. Se actualiza con regularidad y se incluye en el kit de distribución de la aplicación de Kaspersky.

Bases de datos antivirus

Bases de datos que contienen información sobre las amenazas de la seguridad del equipo que conoce Kaspersky en el momento en el que se publican dichas bases de datos antivirus. Las firmas de bases de datos antivirus ayudan a detectar código malicioso en objetos analizados. Los especialistas de Kaspersky crean bases de datos antivirus y estas se actualizan cada hora.

Certificado

Documento electrónico que contiene la clave privada e información sobre el titular de dicha clave y el alcance de esta, y que confirma que la clave pública pertenece al titular. El certificado debe estar firmado por el centro de certificación que lo emitió.

Certificado de la licencia

Un documento que Kaspersky transfiere al usuario junto con el archivo llave o el código de activación. Contiene información sobre la licencia que se concede al usuario.

Clave activa

Clave que utiliza la aplicación actualmente.

Clave adicional

Clave que certifica el derecho a utilizar la aplicación, pero que actualmente no se utiliza.

Cobertura de protección

Objetos que son analizados constantemente por la protección antivirus cuando ésta se ejecuta. Las coberturas de protección de los distintos componentes tienen distintas propiedades.

Cobertura del análisis

Objetos que Kaspersky Endpoint Security analiza mientras realiza una tarea de análisis.

Conector del agente de red

Funcionalidad de la aplicación que conecta la aplicación al agente de red. El agente de red permite la administración remota de la aplicación con Kaspersky Security Center.

Configuración de la aplicación

Configuración de la aplicación común a todos los tipos de tareas y que dirige el funcionamiento global de la aplicación, como la configuración de rendimiento de la aplicación, la de informes y la de respaldo.

Configuración de tareas

Configuración de la aplicación específica para cada tarea.

Cuarentena

Kaspersky Endpoint Security coloca los archivos probablemente infectados en esta carpeta. Los archivos en cuarentena se almacenan en formato cifrado.

Desinfección

Método de procesamiento de objetos infectados que da lugar a la recuperación completa o parcial de datos. No se pueden desinfectar todos los objetos infectados.

Emisor del certificado

El centro de certificación que emitió el certificado.

Exploits

Código de programación que usa una especie de vulnerabilidad en el sistema o software. A menudo los exploits se utilizan para instalar malware en el equipo sin el conocimiento del usuario.

Falsa alarma

Una falsa alarma se produce cuando la aplicación Kaspersky notifica un archivo que no está infectado como infectado, porque la firma del archivo es similar a la de un virus.

Forma normalizada de la dirección de un recurso web

La forma normalizada de la dirección de un recurso web es una representación textual de la dirección de un recurso web obtenido a través de la normalización. La normalización es un proceso mediante el que la representación textual de la dirección de un recurso web cambia de acuerdo con reglas concretas (por ejemplo, exclusión del inicio de sesión HTTP, contraseña y puerto de conexión de la representación textual de la dirección del recurso web; además, la dirección del recurso web cambia de mayúsculas a minúsculas).

En el contexto de la protección antivirus, el fin de la normalización de las direcciones de recursos web consiste en evitar analizar varias veces direcciones de sitios web que puedan diferir en la sintaxis, pese a ser físicamente equivalente.

Ejemplo:

Forma no normalizada de una dirección: `www.Example.com\.`

Forma normalizada de una dirección: `www.example.com.`

Grupo de administración

Un conjunto de dispositivos que comparten funciones comunes y un conjunto de aplicaciones de Kaspersky instaladas en ellos. Los dispositivos se agrupan de modo que se puedan administrar de forma práctica como una sola unidad. Un grupo puede incluir otros grupos. Se pueden crear directivas de grupo y tareas de grupo para cada una de las aplicaciones instaladas en el grupo.

Huella digital del certificado

Información utilizada para identificar una clave de certificado. Una huella digital se crea aplicando una función de hash criptográfica al valor de la clave.

Lista negra de direcciones

Una lista de direcciones de correo electrónico a partir de la cual la aplicación de Kaspersky bloquea todos los mensajes entrantes, independientemente de cuál sea su contenido.

Máscara de archivos

Representación del nombre de un archivo y de su extensión mediante comodines.

Las máscaras de archivos pueden contener cualquier carácter que se permita en los nombres de archivos, incluidos comodines:

- *: Sustituye cero o más caracteres.
- ?: Sustituye a cualquier carácter.

Observe que el nombre y la extensión del archivo se separan siempre con un punto.

Módulo de plataforma segura

Un microchip desarrollado para proporcionar funciones básicas relacionadas con la seguridad (por ejemplo, para almacenar claves de cifrado). Un módulo de plataforma segura se suele instalar en la placa base del ordenador e interactúa con todos los otros componentes del sistema a través del bus de hardware.

Módulos de la aplicación

Los archivos que se incluyen en el archivo de instalación de la aplicación, que implementa la funcionalidad principal de la aplicación. Un módulo ejecutable independiente se corresponde con cada tipo de tarea que realiza la aplicación (Protección en tiempo real, Análisis a pedido y Actualización). Al iniciar un análisis completo del equipo desde la ventana principal de la aplicación, inicia el módulo de esta tarea.

Movimiento de archivos a Cuarentena

Método de gestión de un archivo probablemente infectado mediante el cual se bloquea el acceso al archivo, que se mueve de su ubicación original a la carpeta Cuarentena, donde se mantiene cifrado para descartar la amenaza de infección.

Objeto OLE

Un archivo adjunto o un archivo incrustado en otro archivo. Las aplicaciones de Kaspersky permiten analizar objetos OLE en busca de virus. Por ejemplo, si incluye una tabla de Microsoft Excel® en un documento de Microsoft Office Word, la aplicación analizará la tabla como un objeto OLE.

Parche

Una pequeña adición a la aplicación que soluciona errores descubiertos durante el funcionamiento de la aplicación, o bien instala actualizaciones.

Phishing

Un tipo de fraude en Internet en el cual los mensajes de correo electrónico se envían con el objetivo de robar datos confidenciales. Frecuentemente, suele tratarse de datos bancarios.

Respaldo

Almacenamiento especial de las copias de seguridad de los archivos que se crean antes del inicio de los procesos de desinfección o eliminación.

Servicio de red

Conjunto de parámetros que definen la actividad de red. Para esta actividad de red, puede crear una regla de red que regule el funcionamiento de Firewall.

Servidor de administración

Un componente de Kaspersky Security Center que almacena información de forma centralizada acerca de todas las aplicaciones de Kaspersky que están instaladas en la red corporativa. También puede utilizarse para administrar estas aplicaciones.

Sujeto del certificado

Titular de una clave privada vinculado a un certificado. Puede tratarse de un usuario, aplicación, objeto virtual, equipo o servicio.

Tarea

Funciones realizadas por la aplicación de Kaspersky como tareas, por ejemplo: Protección de archivos de tiempo real, Análisis completo de dispositivo, Actualización de bases de datos.

Información sobre el código de terceros

La información sobre el código de terceros se incluye en el archivo legal_notices.txt, en la carpeta de instalación de la aplicación.

Información de marcas registradas

Todas las marcas registradas y marcas de servicio son propiedad de sus respectivos propietarios.

Adobe, Acrobat y Shockwave son marcas comerciales o marcas registradas de Adobe Systems Incorporated en los EE. UU. y otros países.

Mac y FireWire son marcas registradas de Apple Inc. registradas en los Estados Unidos de América y otros países.

AutoCAD es una marca comercial o marca registrada de Autodesk, Inc. y/o sus filiales o empresas afiliadas en los Estados Unidos y otros países.

La identidad gráfica de Bluetooth y su logotipo son propiedad de Bluetooth SIG, Inc.

Borland es una marca comercial o marca registrada de Borland Software Corporation en los Estados Unidos y otros países.

Citrix y Citrix Provisioning Services son marcas comerciales de Citrix Systems, Inc. y/o sus filiales registradas en la oficina de patentes de los Estados Unidos y otros países.

dBase es una marca de dataBased Intelligence, Inc.

EMC y SecurID son marcas registradas de EMC Corporation o marcas comerciales registradas de EMC Corporation registradas en los EE. UU. y otros países.

ICQ es una marca y/o una marca de servicio de ICQ LLC.

Intel y Pentium son marcas registradas de Intel Corporation en los Estados Unidos de América y otros países.

Logitech es una marca comercial registrada o marca comercial de Logitech Company en los EE. UU. y otros países.

Mail.ru es una marca registrada de Mail.Ru, LLC.

Microsoft, Windows, Internet Explorer, Access, Excel, PowerPoint, Outlook, Outlook Express, Windows Server, Visual Basic, Visual FoxPro, BitLocker, LifeCam Cinema, PowerShell y Surface son marcas registradas de Microsoft Corporation en los Estados Unidos de América y otros países.

Mozilla y Thunderbird son marcas comerciales de Mozilla Foundation.

Novell es una marca comercial de Novell Inc. registrada tanto en Estados Unidos como en otros lugares.

Java y JavaScript son marcas registradas de Oracle Corporation y/o sus filiales.

SafeNet es la marca registrada de SafeNet, Inc.

UNIX es una marca registrada en los Estados Unidos y en otros países, y se utiliza según la licencia de X/Open Company Limited.