KASPERSKY lab

Kaspersky Embedded Systems Security

Guía del administrador

Versión de la aplicación: 2.3.0.754

Estimado usuario:

Gracias por elegir Kaspersky Lab como su proveedor de software de seguridad. Esperamos que este documento le ayude a usar nuestro producto.

Fecha de la revisión del documento: 19.04.2019

https://latam.kaspersky.com
https://support.kaspersky.com/mx/

Contenido

Acerca de esta guía

La Guía del administrador de Kaspersky Embedded Systems Security 2.3 (en adelante, denominada “Kaspersky Embedded Systems Security”, “la aplicación”) está dirigida a los especialistas encargados de instalar y administrar Kaspersky Embedded Systems Security en todos los dispositivos protegidos, y a los especialistas encargados de proporcionar servicio de soporte técnico a organizaciones mediante Kaspersky Embedded Systems Security.

La Guía contiene información acerca de la configuración y el uso de Kaspersky Embedded Systems Security.

La Guía también lo ayudará a conocer las fuentes de información sobre la aplicación y cómo recibir soporte técnico.

En este capítulo

En este documento

La Guía del administrador de Kaspersky Embedded Systems Security contiene las siguientes secciones:

Fuentes de información acerca de Kaspersky Embedded Systems Security

Esta sección enumera las fuentes de información acerca de la aplicación.

Kaspersky Embedded Systems Security

Esta sección describe las funciones, los componentes y el kit de distribución de Kaspersky Embedded Systems Security, además de brindar una lista de requisitos de hardware y software de Kaspersky Embedded Systems Security.

Instalación y desinstalación de la aplicación

Esta sección proporciona instrucciones paso a paso para instalar y eliminar Kaspersky Embedded Systems Security.

Icono de interfaz de la aplicación

Esta sección brinda información sobre los elementos de la interfaz de Kaspersky Embedded Systems Security.

Licencia de la aplicación

Esta sección brinda información sobre los conceptos principales relacionados con el otorgamiento de una licencia de la aplicación.

Cómo iniciar y detener Kaspersky Embedded Systems Security

Esta sección contiene información sobre cómo iniciar y detener el Complemento de administración de Kaspersky Embedded Systems Security (en adelante, denominado Complemento de administración) y el servicio de Kaspersky Security.

Acerca de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security

Esta sección contiene información acerca de los permisos para administrar Kaspersky Embedded Systems Security y los servicios de Windows® registrados por la aplicación, e instrucciones sobre cómo configurar estos permisos.

Creación y configuración de directivas

Esta sección contiene información sobre la utilización de las directivas de Kaspersky Security Center para administrar Kaspersky Embedded Systems Security en diferentes equipos.

Creación y configuración de tareas con Kaspersky Security Center

Esta sección contiene información sobre las tareas de Kaspersky Embedded Systems Security y cómo crearlas, ajustar sus configuraciones, e iniciarlas y detenerlas.

Administración de las configuraciones de la aplicación

Esta sección contiene información acerca de cómo ajustar las configuraciones generales de Kaspersky Embedded Systems Security en Kaspersky Security Center.

Protección del equipo en tiempo real

Esta sección brinda información sobre los componentes de Protección del equipo en tiempo real: Protección de archivos en tiempo real, Uso de KSN y Prevención de exploits. Esta sección también brinda instrucciones sobre cómo configurar tareas de protección del equipo en tiempo real y cómo administrar la configuración de seguridad de un equipo protegido.

Control de actividad local

Esta sección proporciona información sobre la funcionalidad de Kaspersky Embedded Systems Security que controla los inicios de aplicaciones y las conexiones a dispositivos externos mediante USB.

Control de actividad de red

Esta sección contiene la información sobre la tarea de administración de firewall.

Inspección del sistema

Esta sección contiene la información sobre la tarea del Monitor de integridad de archivos y funciones para inspeccionar el registro del sistema operativo.

Integración con sistemas de terceros

Esta sección describe la integración de Kaspersky Embedded Systems Security con funciones y tecnologías de terceros.

Cómo utilizar Kaspersky Embedded Systems Security desde la línea de comandos

Esta sección describe cómo utilizar Kaspersky Embedded Systems Security desde la línea de comandos.

Comunicarse con el soporte técnico

Esta sección describe cómo se puede recibir soporte técnico y las condiciones en las cuales se encuentra disponible.

Glosario

Esta sección contiene la lista de términos que se mencionan en el documento, así como sus definiciones respectivas.

AO Kaspersky Lab

Esta sección proporciona información sobre AO Kaspersky Lab.

Información sobre código de terceros

Esta sección contiene información acerca del código de terceros usado en la aplicación.

Avisos de marcas registradas

Esta sección enumera las marcas comerciales reservadas a propietarios externos que se mencionan en el documento.

Índice

Esta sección le permite encontrar rápidamente la información necesaria en el documento.

Convenciones del documento

Este documento utiliza las siguientes convenciones (consulte la tabla que se encuentra a continuación).

Tabla 1. Convenciones del documento

Texto de ejemplo	Descripción de la convención del documento
Tenga en cuenta que...	Las advertencias están resaltadas en rojo y destacadas en un cuadro. Las advertencias contienen información sobre las acciones que pueden tener consecuencias no deseadas.
Le recomendamos que use...	Las notas están destacadas en un cuadro. Las notas contienen información complementaria y de referencia.
Por ejemplo: …	Los ejemplos se dan en letras de imprenta, con un fondo azul y debajo del título “Por ejemplo”.
Actualización significa... Se produce el evento *Las bases de datos están desactualizadas*.	Los siguientes elementos están en *cursiva* en el texto: • Términos nuevos • Nombres de eventos y estados de las aplicaciones
Presione **ENTER**. Presione **ALT**+**F4**.	Los nombres de las teclas del teclado aparecen en **negrita** y en mayúsculas. Los nombres de teclas conectados por el signo "+" (más) indican el uso de una combinación de teclas. Esas teclas se deben presionar simultáneamente.
Haga clic en el botón **Habilitar**.	Los nombres de los elementos de la interfaz de la aplicación, por ejemplo, cuadros de texto, elementos de menú y botones, están destacados en **negrita**.

Texto de ejemplo	Descripción de la convención del documento
► *Para configurar la programación de una tarea:*	Las frases introductorias de las instrucciones están en cursiva y tienen el símbolo de una flecha.
En la línea de comandos, escriba `help` Aparece el siguiente mensaje: Especifique la fecha en el formato `dd:mm:aa`.	Los siguientes tipos de contenido del texto están destacados con una fuente especial: • Texto en la línea de comandos • Texto de los mensajes que la aplicación muestra en la pantalla • Los datos se deben introducir desde el teclado
<Nombre de usuario>	Las variables se ponen entre corchetes angulares. En lugar del nombre de la variable, se debe insertar el valor correspondiente y omitir los corchetes angulares.

Fuentes de información acerca de Kaspersky Embedded Systems Security

Esta sección enumera las fuentes de información acerca de la aplicación.

Puede seleccionar la fuente de información más adecuada, según el nivel de importancia y la urgencia del problema.

En este capítulo

Fuentes para la recuperación de información independiente

Puede usar las siguientes fuentes para buscar información acerca de Kaspersky Embedded Systems Security:

- Página de Kaspersky Embedded Systems Security en el sitio web de Kaspersky Lab.
- Página de Kaspersky Embedded Systems Security en el sitio web de soporte técnico (base de conocimientos).
- Manuales.

Si no encontró una solución para su problema, póngase en contacto con el Servicio de soporte técnico de Kaspersky Lab https://support.kaspersky.com/mx.

Se requiere una conexión a Internet para usar las fuentes de información en línea.

Página de Kaspersky Embedded Systems Security en el sitio web de Kaspersky Lab

En la página de Kaspersky Embedded Systems Security https://latam.kaspersky.com/enterprise-security/embedded-systems, puede consultar información general acerca de la aplicación, sus funciones y sus características.

La página de Kaspersky Embedded Systems Security contiene un vínculo a la tienda en línea. Allí podrá comprar la aplicación o renovar la licencia.

Página de Kaspersky Embedded Systems Security en la Base de conocimientos

La Base de conocimientos es una sección del sitio web del Servicio de soporte técnico.

La página de Kaspersky Embedded Systems Security en la Base de conocimientos https://support.kaspersky.com/mx/kess2/ incluye artículos que brindan información útil, recomendaciones y respuestas a las preguntas frecuentes sobre cómo comprar, instalar y usar la aplicación.

Los artículos de la base de conocimientos pueden responder preguntas relacionadas no solo con Kaspersky Embedded Systems Security, sino también con otras aplicaciones de Kaspersky Lab. Los artículos de la base de conocimientos también pueden incluir noticias de soporte técnico.

Documentación de Kaspersky Embedded Systems Security

La Guía del administrador de Kaspersky Embedded Systems Security contiene información acerca de la instalación, desinstalación, configuración y uso de la aplicación.

Debate sobre las aplicaciones de Kaspersky Lab en la comunidad

Si su pregunta no requiere una respuesta inmediata, puede analizarla con los expertos de Kaspersky Lab y otros usuarios de nuestra comunidad https://community.kaspersky.com/.

En esta comunidad, puede consultar temas actuales, dejar comentarios y crear temas nuevos.

Kaspersky Embedded Systems Security

Esta sección describe las funciones, los componentes y el kit de distribución de Kaspersky Embedded Systems Security, además de brindar una lista de requisitos de hardware y software de Kaspersky Embedded Systems Security.

En este capítulo

Acerca de Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security protege equipos y otros sistemas integrados que ejecutan Microsoft® Windows contra virus y otras amenazas del equipo. Los usuarios de Kaspersky Embedded Systems Security son administradores de red corporativos y especialistas a cargo de la protección antivirus de la red corporativa.

Puede instalar Kaspersky Embedded Systems Security en diversos sistemas integrados que ejecuten Windows, incluidos los siguientes tipos de dispositivos:

- Cajeros automáticos;
- TPV (terminal de punto de venta).

Kaspersky Embedded Systems Security se puede administrar de las siguientes formas:

- Mediante la Consola de la aplicación instalada en el mismo equipo donde está instalado Kaspersky Embedded Systems Security o en un equipo diferente.
- Mediante comandos en la línea de comandos.
- Mediante la Consola de administración de Kaspersky Security Center.

La aplicación Kaspersky Security Center también se puede utilizar para la administración centralizada de varios equipos que ejecutan Kaspersky Embedded Systems Security.

Es posible revisar los contadores de rendimiento de Kaspersky Embedded Systems Security para la aplicación "Supervisor del sistema", además de los contadores y las capturas SNMP.

Componentes y funciones de Kaspersky Embedded Systems Security

La aplicación incluye los siguientes componentes:

- **Protección en tiempo real**. Kaspersky Embedded Systems Security analiza los objetos cuando obtiene acceso a ellos. Kaspersky Embedded Systems Security analiza los siguientes objetos:
  - Archivos
  - Flujos de sistemas de archivos alternativos (flujos NTFS)
  - Registros de inicio maestro y sectores de inicio de los discos duros locales y los discos extraíbles
- **Análisis a pedido**. Kaspersky Embedded Systems Security ejecuta un solo análisis de la zona especificada en busca de virus y otras amenazas de seguridad informática. La aplicación analiza archivos, RAM y objetos de ejecución automática en un equipo protegido.
- **Control de inicio de aplicaciones**. El componente rastrea los intentos de los usuarios de iniciar aplicaciones y controla los inicios de la aplicación en un equipo protegido.
- **Control de dispositivos**. El componente controla el registro y el uso de dispositivos del almacenamiento y unidades de CD/DVD a fin de proteger el equipo contra amenazas de seguridad informática que pueden surgir al intercambiar archivos con unidades flash conectadas mediante USB u otros tipos de dispositivos externos.
- **Administración de firewall**. Este componente proporciona la capacidad de administrar el firewall de Windows: configurar los ajustes y reglas de firewall del sistema operativo, y bloquear toda posibilidad de configuración externa del firewall.
- **Monitor de integridad de archivos**. Kaspersky Embedded Systems Security detecta cambios en los archivos dentro de las áreas de supervisión especificadas en la configuración de la tarea. Estos cambios pueden indicar una violación de la seguridad en el equipo protegido.
- **Inspección de registros**. Este componente supervisa la integridad del ambiente protegido sobre la base de los resultados de una inspección de los registros de eventos de Windows.

Las siguientes funciones se implementan en la aplicación:

- **Actualización de bases de datos y actualización de módulos del programa**. Kaspersky Embedded Systems Security descarga las actualizaciones de las bases de datos y los módulos de la aplicación desde los servidores de actualizaciones FTP o HTTP de Kaspersky Lab, el servidor de administración de Kaspersky Security Center u otros orígenes de actualizaciones.
- **Cuarentena**. Kaspersky Embedded Systems Security pone en cuarentena los objetos probablemente infectados al pasarlos de su ubicación original a la carpeta de *Cuarentena*. Por razones de seguridad, los objetos son puestos en la carpeta de Cuarentena en forma cifrada.
- **Copia de seguridad**. Kaspersky Embedded Systems Security almacena copias cifradas de los objetos clasificados como *Infectados* en *Copia de seguridad* antes de desinfectarlos o eliminarlos.
- **Notificaciones de administrador y usuario**. Puede configurar la aplicación para que notifique al administrador y a los usuarios que tienen acceso al equipo protegido sobre eventos en el funcionamiento de Kaspersky Embedded Systems Security y el estado de la protección antivirus del equipo.
- **Cómo importar y exportar la configuración**. Puede exportar la configuración de Kaspersky Embedded Systems Security a un archivo de configuración XML e importar los parámetros a Kaspersky Embedded Systems Security desde el archivo de configuración. Puede guardar todos los ajustes de la aplicación o únicamente los ajustes de componentes individuales a un archivo de configuración.
- **Aplicar plantillas**. Puede configurar manualmente los ajustes de seguridad de un nodo en el árbol o en una lista de recursos del archivo del equipo y guardar los valores de ajuste configurados como plantilla. Esta plantilla se puede utilizar entonces para configurar las opciones de seguridad de otros nodos en las

tareas de análisis y protección de Kaspersky Embedded Systems Security.

- **Administración de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security**. Puede configurar los derechos de administración de Kaspersky Embedded Systems Security y de los servicios de Windows que están registrados por la aplicación, para usuarios y grupos de usuarios.
- **Carga de eventos en el registro de eventos de la aplicación**. Kaspersky Embedded Systems Security registra la información sobre la configuración de los componentes del software, el estado actual de las tareas, los eventos que ocurrieron durante su ejecución, los eventos asociados con la administración de Kaspersky Embedded Systems Security y la información necesaria para el diagnóstico de errores en Kaspersky Embedded Systems Security.
- **Zona de confianza**. Puede generar una lista de objetos que desea excluir de la protección o del área del análisis que Kaspersky Embedded Systems Security aplicará durante las tareas de análisis a pedido y protección en tiempo real.
- **Prevención de exploits**. Puede proteger la memoria de proceso de exploits mediante un Agente inyectado en el proceso.

Novedades

Kaspersky Embedded Systems Security ofrece las siguientes mejoras y funciones nuevas:

- Compatibilidad con nuevas versiones de sistemas operativos Microsoft Windows.

  Windows 10 Redstone 6 (x32 y x64).

- No puede verse el código de activación completo en la aplicación GUI.

  El código de activación que se añadió está parcialmente escondido cuando aparece en la aplicación GUI, y ningún usuario puede verlo completamente.

Kit de distribución

El kit de distribución incluye la aplicación de bienvenida que le permite realizar lo siguiente:

- Iniciar el asistente de instalación de Kaspersky Embedded Systems Security.
- Iniciar el asistente de instalación de la Consola de Kaspersky Embedded Systems Security.
- Iniciar el asistente que instalará el Complemento de administración de Kaspersky Embedded Systems Security para administrar la aplicación mediante Kaspersky Security Center.
- Leer la Guía del administrador.
- Ir a la página de Kaspersky Embedded Systems Security en el sitio web de Kaspersky Lab.
- Visitar el sitio web de soporte técnico https://support.kaspersky.com/mx/.
- Leer información sobre la versión actual de Kaspersky Embedded Systems Security.

La carpeta \console contiene archivos para instalar la Consola de la aplicación (el conjunto de componentes de “Herramientas de administración de Kaspersky Embedded Systems Security”).

La carpeta \product contiene:

- Archivos para la instalación de los componentes de Kaspersky Embedded Systems Security en un equipo

que ejecuta un sistema operativo de Microsoft Windows de 32 o 64 bits.

- Archivo para la instalación del Complemento de administración de Kaspersky Embedded Systems Security mediante Kaspersky Security Center.
- Archivo que contiene las bases de datos antivirus actuales al momento del lanzamiento de la aplicación.
- Archivo que contiene los términos del Contrato de licencia de usuario final y la Política de privacidad.

La carpeta \product_no_avbases contiene archivos de instalación de los componentes de Kaspersky Embedded Systems Security y del Complemento de administración sin las bases de datos antivirus.

La carpeta \setup contiene los archivos de inicio del programa de bienvenida.

Los archivos del kit de distribución se almacenan en carpetas diferentes según el uso deseado (ver la tabla a continuación).

Tabla 2. Archivos del kit de distribución de Kaspersky Embedded Systems Security

Archivo	Objetivo
autorun.inf	Archivo de ejecución automática del asistente de instalación de Kaspersky Embedded Systems Security para instalar la aplicación desde medios extraíbles.
ess_admin_guide_es.pdf	Guía del administrador.
release_notes.txt	El archivo contiene información sobre la versión.
setup.exe	Archivo de inicio del programa de bienvenida (inicia setup.hta).
\console\esstools_x86(x64).msi	Paquete de Windows Installer; instala la Consola de la aplicación en el equipo protegido.
\console\setup.exe	El archivo que ejecuta el asistente de configuración para el conjunto de componentes de “Herramientas de administración” (incluida la Consola de la aplicación); inicia el archivo del paquete de instalación esstools.msi con la configuración especificada en el asistente de configuración.
\product\bases.cab	Archivo de almacenamiento que contiene las bases de datos antivirus actuales al momento del lanzamiento de la aplicación.
\product\setup.exe	El archivo para instalar Kaspersky Embedded Systems Security en el equipo protegido por medio del asistente; comienza el archivo del paquete de instalación ess.msi con la configuración de instalación especificada en el asistente.
\product\ess_x86(x64).msi	Paquete de Windows Installer; instala Kaspersky Embedded Systems Security en el equipo protegido.
\product\ess.kud	Archivo en el formato definición Unicode de Kaspersky con una descripción del paquete de instalación para la instalación remota de Kaspersky Embedded Systems Security mediante Kaspersky Security Center.
\product\klcfginst.exe	Instalador de un Complemento de administración de Kaspersky Embedded Systems Security mediante Kaspersky Security Center. Instale el Complemento de administración en cada equipo donde encuentra instalada la Consola de administración de Kaspersky Security Center si planea usarla para administrar Kaspersky Embedded Systems Security.
\product\license.txt	Texto del Contrato de licencia de usuario final y la Política de privacidad.

Archivo	Objetivo
\product\migration.txt	El archivo describe la migración desde versiones anteriores de la aplicación.
\setup\setup.hta	Archivo de inicio del programa de bienvenida.

Requisitos de hardware y software

Antes de instalar Kaspersky Embedded Systems Security, debe desinstalar otras aplicaciones antivirus del equipo.

Requisitos de software para el equipo protegido

Puede instalar Kaspersky Embedded Systems Security en un equipo que ejecute un sistema operativo Microsoft Windows de 32 o 64 bits.

Se necesita tener Windows Installer 3.1 para una instalación correcta de la aplicación que funcione en un equipo que ejecuta Microsoft Windows XP.

Para instalar y usar Kaspersky Embedded Systems Security en los equipos con sistemas operativos integrados, se requiere el componente de administración de filtros.

Puede instalar Kaspersky Embedded Systems Security en un equipo que ejecute alguno de los siguientes sistemas operativos Microsoft Windows de 32 o 64 bits:

- Windows XP Embedded SP3 (32 bits)
- Windows Embedded POSReady 2009 (32 bits)
- Windows XP Professional SP2/SP3 (32 bits, 64 bits)
- Windows Embedded Standard 7 SP1 (32 bits, 64 bits)
- Windows Embedded Enterprise 7 SP1 (32 bits, 64 bits)
- Windows Embedded POSReady 7 (32 bits, 64 bit)
- Windows 7 Professional/Enterprise SP1 (32 bits, 64 bits)
- Windows Embedded 8.1 Industry Professional/Enterprise (32 bits, 64 bits)
- Windows Embedded 8.0 Standard (32 bits, 64 bits)
- Windows 8 Professional/Enterprise (32 bits, 64 bits)
- Windows 8.1 Professional/Enterprise (32 bits, 64 bits)
- Windows 10 Professional/Enterprise (32 bits, 64 bits)

- Windows 10 IoT Enterprise (32 bits, 64 bits)
- Windows 10 Redstone 1 Professional/Enterprise/IoT Enterprise (32 bits, 64 bits)
- Windows 10 Redstone 2 Professional/Enterprise/IoT Enterprise (32 bits, 64 bits)
- Windows 10 Redstone 3 Professional/Enterprise/IoT Enterprise (32 bits, 64 bits)
- Windows 10 Redstone 4 Professional/Enterprise/IoT Enterprise (32 bits, 64 bits)
- Windows 10 Redstone 5 Professional/Enterprise/IoT Enterprise (32 bits, 64 bits)
- Windows 10 Redstone 6 Professional/Enterprise/IoT Enterprise (32 bits, 64 bits)

Requisitos de hardware para el equipo protegido

Los requisitos del hardware para el equipo protegido varían según el sistema operativo Windows instalado:

- Requisitos del hardware para un equipo con sistema operativo Windows XP (32/64 bits), Windows 7 (32 bits), Windows 8 (32 bits), Windows Embedded XP, Windows Embedded POSReady 2009 o Windows Embedded POSReady 7:
  - Configuración mínima:
    - Requisitos de espacio de disco:
      - Para instalar el componente del Control de inicio de aplicaciones: 50 MB.
      - Para instalar todos los componentes de Kaspersky Embedded Systems Security: 2 GB
    - RAM:
      - 256 MB para instalar solo el componente Control de inicio de aplicaciones en el equipo con el sistema operativo Microsoft Windows.
      - 512 MB para realizar la instalación completa de todos los componentes.
    - Requisitos del procesador:
      - para sistemas operativos Microsoft Windows de 32 bits: Procesador de núcleo único de 1,4 GHz Intel® Pentium® III.
      - para sistemas operativos Microsoft Windows de 64 bits: Procesador de núcleo único de 1,4 GHz Pentium IV.
  - Configuración recomendada:
    - Requisitos de espacio de disco:
      - Para instalar el componente del Control de inicio de aplicaciones: 2 GB.
      - Para instalar todos los componentes de Kaspersky Embedded Systems Security: 4 GB
    - RAM: 2 GB
    - Requisitos del procesador: procesador cuatro núcleos de 2,4 GHz.

- Requisitos del hardware para un equipo con sistema operativo Windows 7 (64 bits), Windows 8 (64 bits), Windows 10 (64 bits), Windows Embedded 7, o Windows Embedded 8:
  - Configuración mínima:
    - Requisitos de espacio de disco:
      - Para instalar el componente del Control de inicio de aplicaciones: 50 MB.
      - Para instalar todos los componentes de Kaspersky Embedded Systems Security: 2 GB
    - RAM: 1 GB
    - Requisitos del procesador:
      - para sistemas operativos Microsoft Windows de 32 bits: Procesador de núcleo único de 1,4 GHz Pentium III.
      - para sistemas operativos Microsoft Windows de 64 bits: Procesador de núcleo único de 1,4 GHz Pentium IV.
  - Configuración recomendada
    - Requisitos de espacio de disco:
      - Para instalar el componente del Control de inicio de aplicaciones: 2 GB.
      - Para instalar todos los componentes de Kaspersky Embedded Systems Security: 4 GB
    - RAM: 2 GB
    - Requisitos del procesador: procesador cuatro núcleos de 2,4 GHz.

Requisitos funcionales y limitaciones

Esta sección describe los requisitos funcionales adicionales y las limitaciones existentes de los componentes de Kaspersky Embedded Systems Security.

En esta sección

Instalación y desinstalación

- Durante la instalación de la aplicación es posible que aparezca una advertencia indicando si una nueva ruta a la carpeta de instalación de Kaspersky Embedded Systems Security contiene más de 150 símbolos. La advertencia no afecta el proceso de instalación: Kaspersky Embedded Systems Security se instalará y ejecutará correctamente.
- Para la instalación del componente de compatibilidad con el protocolo SNMP, se debe reiniciar el servicio

SNMP (si se está ejecutando).

- Para la instalación y el funcionamiento de Kaspersky Embedded Systems Security en el dispositivo administrado por el sistema operativo integrado, se debe instalar el componente de administración de filtros.
- La instalación de las herramientas de administración de Kaspersky Embedded Systems Security no está disponible mediante las directivas del grupo de Microsoft Active Directory®.
- Al instalar la aplicación en equipos que ejecutan los sistemas operativos más antiguos, que no pueden recibir actualizaciones periódicas, se debe comprobar que cuenten con los siguientes certificados raíz: DigiCert Assured ID Root CA, DigiCert_High_Assurance_EV_Root_CA, DigiCertAssuredIDRootCA. La ausencia de dichos certificados puede provocar un funcionamiento incorrecto de la aplicación. Se recomienda instalar los certificados especificados de cualquier manera posible.
- La consola de Kaspersky Embedded Systems Security no se puede desinstalar mediante el menú **Iniciar**. Puede desinstalar la consola Kaspersky Embedded Systems Security con el vínculo de la ventana Agregar o quitar programas.

Monitor de integridad de archivos

De forma predeterminada, el Monitor de integridad de archivos no supervisa cambios en las carpetas del sistema ni en los archivos de optimización y limpieza del sistema. De esta forma evita que el informe de la tarea contenga información sobre cambios rutinarios en los archivos, aquellos que el sistema operativo realiza de forma constante. El usuario no puede incluir tales carpetas en el área de supervisión de forma manual.

Las siguientes carpetas y archivos están excluidas del área de supervisión:

- Archivos NTFS de limpieza y optimización con id de archivo de 0 a 33
- "%SystemRoot%\\Prefetch\\"
- "%SystemRoot%\\ServiceProfiles\\LocalService\\AppData\\Local\\"
- "%SystemRoot%\\System32\\LogFiles\\Scm\\"
- "%SystemRoot%\\Microsoft.NET\\Framework\\v4.0.30319\\"
- "%SystemRoot%\\Microsoft.NET\\Framework64\\v4.0.30319\\"
- "%SystemRoot%\\Microsoft.NET\\"
- "%SystemRoot%\\System32\\config\\"
- "%SystemRoot%\\Temp\\"
- "%SystemRoot%\\ServiceProfiles\\LocalService\\"
- "%SystemRoot%\\System32\\winevt\\Logs\\"
- "%SystemRoot%\\System32\\wbem\\repository\\"
- "%SystemRoot%\\System32\\wbem\\Logs\\"
- "%ProgramData%\\Microsoft\\Windows\\WER\\ReportQueue\\"
- "%SystemRoot%\\SoftwareDistribution\\DataStore\\"
- "%SystemRoot%\\SoftwareDistribution\\DataStore\\Logs\\"
- "%ProgramData%\\Microsoft\\Windows\\AppRepository\\"
- "%ProgramData%\\Microsoft\\Search\\Data\\Applications\\Windows\\"

- "%SystemRoot%\\Logs\\SystemRestore\\"
- "%SystemRoot%\\System32\\Tasks\\Microsoft\\Windows\\TaskScheduler\\"

La aplicación excluye carpetas de niveles superiores.

El componente no supervisa los cambios de archivo si se evita el sistema de archivos ReFS o NTFS (es decir, que los cambios se realicen a través de BIOS, LiveCD, entre otros).

Administración de firewall

- El funcionamiento con direcciones IP en formato IPv6 no está disponible cuando el área especificada de la regla aplicada contiene una única dirección.
- Las reglas de la directiva de Firewall predeterminadas permiten la ejecución de los escenarios básicos de interacción entre equipos locales y el Servidor de administración. Para el uso completo de las funciones del Kaspersky Security Center, se deben configurar reglas para puertos de forma manual. La información sobre números de puertos, protocolos y sus funciones se incluye en la base de conocimientos de Kaspersky Security Center (ID del artículo: 9297).
- Si reglas de firewall de Windows y los grupos de reglas no se agregaron a la configuración de la tarea al instalar la aplicación, la aplicación no controlará la modificación de dichas reglas durante las revisiones minuciosas de la tarea de administración de Firewall. Para actualizar el estado e incluir tales reglas, se debe reiniciar la tarea de administración del Firewall.
- Cuando la tarea de Administración del Firewall se inicia, los siguientes tipos de reglas son automáticamente eliminados desde la configuración del firewall del sistema operativo:
  - regla de denegación;
  - reglas de supervisión del tráfico de salida.

Otras limitaciones

Análisis a pedido, protección de archivos en tiempo real:

- El análisis de dispositivos MTP no está disponible.
- El análisis de objetos del archivo no está disponible si no se habilita el análisis de archivos SFX, si el análisis de archivos está habilitado en la configuración de protección de Kaspersky Embedded Systems Security, la aplicación analiza automáticamente los objetos tanto en archivos como en archivos SFX. También es posible analizar únicamente archivos SFX.

Licencia:

- la activación de la aplicación con la clave a través del asistente de configuración no estará disponible si la clave está almacenada en el disco (que se creó con el comando SUBST) o si se especifica la ruta de red al archivo de clave.

Actualizaciones:

- después de la instalación de las actualizaciones de módulos críticas de Kaspersky Embedded Systems Security, el icono de la aplicación se esconde de forma predeterminada.
- KLRAMDISK no se admite en equipos que se ejecutan con los sistemas operativos Windows XP y

Windows 2003.

Interfaz:

- Si usa el filtrado de la Consola de la aplicación en las tarea de cuarentena, copia de seguridad, registro de auditoría del sistema o registro de tareas, se debe conservar el uso de mayúsculas y minúsculas.
- Puede usar solo una máscara y únicamente al final de la ruta, cuando configure la protección o el área del análisis en la Consola de la aplicación. Ejemplos de uso correcto de la máscara: “C:\Temp\Temp*" o "C:\Temp\Temp???.doc" o "C:\Temp\Temp*.doc". La limitación no afecta la configuración de la Zona de confianza.

Seguridad:

- Si el Control de la cuenta de usuario en la configuración del sistema operativo está activado, una cuenta de usuario debe formar parte del grupo de Administradores KAVWSEE para abrir la Consola de la aplicación con un doble clic en el icono de la aplicación ubicado en la zona de notificaciones de la bandeja. En otro caso, será necesario iniciar sesión como usuario, lo que permite abrir la Interfaz de diagnóstico compacto o el complemento Microsoft Management Console.
- La desinstalación de la aplicación mediante la ventana **Programas y funciones** de Microsoft Windows no está disponible si el Control de la cuenta de usuario está activado.

Integración con Kaspersky Security Center:

- El Servidor de administración verifica la validez de las actualizaciones de bases de datos al recibir los paquetes de actualización y antes de enviar las actualizaciones a los equipos de la red. El Servidor de administración no verifica la validez de las actualizaciones recibidas del módulo del software.
- Asegúrese de que las casillas requeridas estén seleccionadas en la configuración de Interacción con Servidor de administración. Debe hacerlo al momento de utilizar los componentes que transmiten los datos dinámicamente modificados a Kaspersky Security Center con la ayuda de las listas de la red (Cuarentena, Copia de seguridad).

Prevención de exploits:

- La prevención de exploits no está disponible si las bibliotecas apphelp.dll no están cargadas en la configuración del entorno actual.
- El componente de prevención de exploits es incompatible con la herramienta EMET de Microsoft en equipos que ejecutan el sistema operativo Microsoft Windows 10: Kaspersky Embedded Systems Security bloquea EMET si el componente de prevención de exploits se instala en un equipo que cuenta con EMET.

Instalación y desinstalación de la aplicación

Esta sección proporciona instrucciones paso a paso para instalar y eliminar Kaspersky Embedded Systems Security.

En este capítulo

Códigos de los componentes del software Kaspersky Embedded Systems Security para el servicio Windows Installer

De forma predeterminada, los archivos \product\ess_x86.msi y \product\ess_x64.ms están diseñados para instalar todos los componentes de Kaspersky Embedded Systems Security. Puede instalar estos componentes al incluirlos en la instalación personalizada.

Los archivos \console\esstools_x86.msi y \console\esstools_x64.msi instalan todos los componentes del software que están incluidos en el conjunto de "Herramientas de administración".

Las siguientes secciones presentan los códigos de los componentes de Kaspersky Embedded Systems Security para el servicio Windows Installer. Estos códigos pueden utilizarse para definir una lista de los componentes que se instalan durante la instalación de Kaspersky Embedded Systems Security desde la línea de comandos.

En esta sección

Componentes de software de Kaspersky Embedded Systems Security

La siguiente tabla contiene los códigos y las descripciones de los componentes de software de Kaspersky Embedded Systems Security.

Tabla 3. Descripción de los componentes de la aplicación Kaspersky Embedded Systems Security

Componente	Identificador	Funciones realizadas
Funcionalidad básica	Core	Este componente contiene el conjunto de funciones básicas de la aplicación y garantiza su operación.
Control de inicio de aplicaciones	AppCtrl	Este componente supervisa los intentos del usuario de ejecutar aplicaciones y autoriza o deniega el inicio de estas de acuerdo con las reglas de Control de inicio de aplicaciones especificadas. Se implementa en la tarea de Control de inicio de aplicaciones.
Control de dispositivos	DevCtrl	Este componente supervisa los intentos de conectar dispositivos de almacenamiento mediante USB a un equipo protegido y permite o restringe el uso de estos dispositivos según las reglas de control de dispositivos especificadas. El componente se implementa en la tarea de Control de dispositivos.
Protección antivirus	AVProtection	Este componente proporciona la protección antivirus y contiene los siguientes componentes: • Análisis a pedido • Protección de archivos en tiempo real
Análisis a pedido	Ods	Este componente instala los archivos de sistema de Kaspersky Embedded Systems Security y brinda las tareas de análisis a pedido (analiza los objetos del equipo protegido previa solicitud). Si se especifican otros componentes de Kaspersky Embedded Systems Security durante la instalación de Kaspersky Embedded Systems Security desde la línea de comandos, pero no se indica el componente Core, este se instala automáticamente.
Protección de archivos en tiempo real	Oas	Este componente realiza un análisis antivirus de los archivos en el equipo protegido cuando obtiene acceso a estos. Implementa la tarea de Protección de archivos en tiempo real.
Uso de Kaspersky Security Network	Ksn	Este componente brinda protección a partir de las tecnologías en la nube de Kaspersky Lab. Implementa la tarea de Uso de KSN (envío de solicitudes y recepción de conclusiones del servicio de Kaspersky Security Network).

Componente	Identificador	Funciones realizadas
Monitor de integridad de archivos	Fim	Este componente registra las operaciones realizadas en los archivos con el área de supervisión especificada. El componente implementa la tarea Monitor de integridad de archivos.
Prevención de exploits	AntiExploit	Este componente hace posible administrar la configuración para proteger la memoria usada por procesos en la memoria de un equipo protegido.
Administración de firewall	Firewall	Este componente hace posible administrar el firewall de Windows a través de la interfaz gráfica de usuario de Kaspersky Embedded Systems Security. El componente implementa la tarea Administración de firewall.
Módulo de integración con el Agente de red de Kaspersky Security Center	AKIntegration	Este componente proporciona una conexión entre Kaspersky Embedded Systems Security y el Agente de red de Kaspersky Security Center. Puede instalar este componente en el equipo protegido si desea administrar la aplicación a través de Kaspersky Security Center.
Inspección de registros	LogInspector	Este componente supervisa la integridad del ambiente protegido sobre la base de los resultados de una inspección de los registros de eventos de Windows.
Conjunto de contadores de rendimiento del "Supervisor del sistema"	PerfMonCounters	Este componente instala un conjunto de contadores de rendimiento del Supervisor del sistema. Los contadores de rendimiento permiten medir el rendimiento de Kaspersky Embedded Systems Security e identificar posibles cuellos de botella en el equipo cuando Kaspersky Embedded Systems Security se utiliza junto con otros programas.
Contadores y capturas SNMP	SnmpSupport	Este componente publica los contadores y las capturas de Kaspersky Embedded Systems Security a través del Protocolo simple de administración de redes (SNMP) en Microsoft Windows. Este componente puede instalarse en el equipo protegido únicamente si el servicio SNMP de Microsoft está instalado en el mismo equipo.
Icono de Kaspersky Embedded Systems Security en el área de notificación	TrayApp	Este componente muestra el icono de Kaspersky Embedded Systems Security en el área de notificación de la bandeja de tareas del equipo protegido. El icono de Kaspersky Embedded Systems Security muestra el estado de protección del equipo y se puede utilizar para abrir la Consola de Kaspersky Embedded Systems Security en Microsoft Management Console (si está instalada) y la ventana **Acerca de la aplicación**.

Conjunto de “Herramientas administrativas” de los componentes de software

La siguiente tabla contiene los códigos y las descripciones del conjunto de “Herramientas de administración” de los componentes de software.

Tabla 4. Descripción de los componentes de software de las "Herramientas de administración"

Componente	Código	Funciones del componente
Componentes de Kaspersky Embedded Systems Security	MmcSnapin	Este componente instala el complemento Microsoft Management Console mediante la Consola de Kaspersky Embedded Systems Security. Si se especifican otros componentes durante la instalación de las "Herramientas de administración" desde la línea de comandos y no se indica el componente MmcSnapin, este se instala automáticamente.
Help	Help	Este es un archivo de ayuda .chm que se guarda en la carpeta junto con los archivos de las Herramientas de administración de Kaspersky Embedded Systems Security. Puede abrir el archivo de Ayuda a través del menú **Iniciar** o al hacer clic en la tecla **F1** con la ventana de la Consola de la aplicación abierta.
Documentación	Help	Kaspersky Embedded Systems Security agrega un acceso directo al sitio web de Kaspersky Lab, donde está disponible la Guía del administrador en formato PDF. El acceso directo está disponible en el menú **Iniciar**.

Cambios en el sistema después de la instalación de Kaspersky Embedded Systems Security

Si Kaspersky Embedded Systems Security y el conjunto de “Herramientas de administración” (incluida la Consola de la aplicación) se instalan juntos, el servicio Windows Installer realizará las siguientes modificaciones en el equipo:

- Se crean las carpetas de Kaspersky Embedded Systems Security en el equipo protegido y en el equipo donde se instala la Consola de la aplicación.
- Se registran los servicios de Kaspersky Embedded Systems Security.
- Se crea un grupo de usuarios de Kaspersky Embedded Systems Security.
- Las claves de Kaspersky Embedded Systems Security se graban en el registro del sistema.

Estos cambios se describen a continuación.

Carpetas de Kaspersky Embedded Systems Security en un equipo protegido

Cuando se instala Kaspersky Embedded Systems Security, se crean las siguientes carpetas en un equipo protegido:

- La carpeta de instalación predeterminada de Kaspersky Embedded Systems Security que contiene los

archivos ejecutables de Kaspersky Embedded Systems Security depende del conjunto de bits del sistema operativo. Por lo tanto, las carpetas de instalación predeterminadas son las siguientes:

  - En la versión de 32 bits de Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
  - En la versión de 64 bits de Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

- Archivos MIB (Management Information Base) que contienen una descripción de los contadores y los enlaces publicados por Kaspersky Embedded Systems Security a través del protocolo SNMP:
  - %Kaspersky Embedded Systems Security%\mibs
- Las versiones de 64 bits de los archivos ejecutables de Kaspersky Embedded Systems Security (esta carpeta se creará únicamente durante la instalación de Kaspersky Embedded Systems Security para la versión de 64 bits de Microsoft Windows):
  - %Kaspersky Embedded Systems Security%\x64
- Archivos de servicio de Kaspersky Embedded Systems Security:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Data\
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Settings\
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Dskm\
- Archivos con configuración para orígenes de actualizaciones:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Update\
- Actualizaciones de bases de datos y módulos del programa descargados mediante la tarea Copia de actualizaciones (la carpeta se crea la primera vez que se descargan actualizaciones con la tarea Copia de actualizaciones):
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Update\Distribution\
- Registros de tareas y registro de auditoría del sistema:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports\
- Conjunto de bases de datos actualmente en uso:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Current\
- Copias de seguridad de bases de datos; se sobrescriben cada vez que se actualizan las bases de datos:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Backup\
- Archivos temporales creados durante la ejecución de tareas de actualización:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Temp\

- Objetos en cuarentena (carpeta predeterminada):
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\ 2.3\Quarantine\
- Objetos en copia de seguridad (carpeta predeterminada):
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\ 2.3\Backup\
- Objetos restaurados de la copia de seguridad y la cuarentena (carpeta predeterminada para los objetos restaurados):
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\ 2.3\Restored\

Carpeta creada durante la instalación de la Consola de la aplicación

Las carpetas de instalación predeterminadas de la Consola de la Aplicación que contienen los archivos de las "Herramientas de administración" dependen del conjunto de bits del sistema operativo. Por lo tanto, las carpetas de instalación predeterminadas son las siguientes:

- En la versión de 32 bits de Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\
- En la versión de 64 bits de Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\

Servicios de Kaspersky Embedded Systems Security

Los siguientes servicios de Kaspersky Embedded Systems Security se inician con la cuenta de sistema local (SYSTEM):

- Servicio de Kaspersky Security (KAVFS): servicio esencial de Kaspersky Embedded Systems Security que administra las tareas y el flujo de trabajo de Kaspersky Embedded Systems Security.
- Servicio de Kaspersky Security Management (KAVFSGT): este servicio está previsto para la administración de la aplicación Kaspersky Embedded Systems Security a través de la Consola de la Aplicación.
- Servicio de Kaspersky Security Exploit Prevention (KAVFSSLP): un servicio que actúa como intermediario para comunicar la configuración de la seguridad a agentes de seguridad externos y recibir datos sobre eventos de seguridad.

Grupo de Kaspersky Embedded Systems Security

Administradores de ESS es un grupo del equipo protegido, cuyos usuarios disponen de acceso absoluto al servicio de Kaspersky Security Management y a todas las funciones de Kaspersky Embedded Systems Security.

Claves de registro del sistema

Cuando se instala Kaspersky Embedded Systems Security, se crean las siguientes claves de registro del sistema:

- Propiedades de Kaspersky Embedded Systems Security: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Configuración del registro de eventos de Kaspersky Embedded Systems Security (registro de eventos de Kaspersky): [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Propiedades del servicio de administración de Kaspersky Embedded Systems Security: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- Configuración del contador de rendimiento:
  - En la versión de 32 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - En la versión de 64 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- Configuración del componente de compatibilidad con el protocolo SNMP:
  - En la versión de 32 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\SnmpAgent]
  - En la versión de 64 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\SnmpAgent]
- Configuración del archivo de volcado:
  - En la versión de 32 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\CrashDump]
  - En la versión de 64 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\CrashDump]
- Configuración del archivo de rastreo:
  - En la versión de 32 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\Trace]
  - En la versión de 64 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Trace]
- Configuración de las tareas y las funciones de la aplicación: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Environment]

Procesos de Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security inicia los procesos que se describen en la siguiente tabla.

Tabla 5. Procesos de Kaspersky Embedded Systems Security

Nombre de archivo	Objetivo
kavfswp.exe	Flujo de trabajo de Kaspersky Embedded Systems Security
kavtray.exe	Proceso para el icono de la bandeja del sistema
kavfsmui.exe	Proceso para el componente de interfaz de diagnóstico compacto

Nombre de archivo	Objetivo
kavshell.exe	Proceso de la utilidad de línea de comandos
kavfsrcn.exe	Proceso de administración remota de Kaspersky Embedded Systems Security
kavfs.exe	Proceso del servicio de Kaspersky Security
kavfsgt.exe	Proceso del servicio de Kaspersky Security Management
kavfswh.exe	Proceso del servicio de Kaspersky Security Exploit Prevention

Configuraciones de instalación y desinstalación y opciones de la línea de comandos para el servicio de Windows Installer

Esta sección contiene descripciones de las configuraciones para instalar y desinstalar Kaspersky Embedded Systems Security, sus valores predeterminados, claves para modificar la configuración de instalación y sus posibles valores. Estas claves pueden utilizarse junto con claves estándar para el comando `msiexec` del servicio Windows Installer durante la instalación de Kaspersky Embedded Systems Security desde la línea de comandos.

Configuración de instalación y opciones de la línea de comandos en Windows Installer

- Aceptación de los términos del Contrato de licencia de usuario final: debe aceptar los términos para instalar Kaspersky Embedded Systems Security.

  Los valores posibles para la opción de la línea de comandos `EULA=<valor>` son los siguientes:

  - `0`: rechaza los términos del Contrato de licencia de usuario final (valor predeterminado).
  - `1`: acepta los términos del Contrato de licencia de usuario final.

- Aceptación de los términos de la Política de privacidad: debe aceptar los términos para instalar Kaspersky Embedded Systems Security.

  Los valores posibles para la opción de la línea de comandos `PRIVACYPOLICY=<valor>` son los siguientes:

  - `0`: rechaza los términos de la Política de privacidad (valor predeterminado).
  - `1`: acepta los términos de la Política de privacidad.

- Instalación de Kaspersky Embedded Systems Security con un análisis preliminar de los procesos activos y los sectores de inicio de los discos locales

  Los valores posibles para la opción de la línea de comandos `PRESCAN=<valor>` son los siguientes:

  - `0`: no realice un análisis preliminar de los procesos activos y de los sectores de arranque de los discos locales durante la instalación (valor predeterminado).
  - `1`: realice un análisis preliminar de los procesos activos y de los sectores de arranque de los discos locales durante la instalación.

- Carpeta de destino en la que se guardan los archivos de Kaspersky Embedded Systems Security durante la instalación. Puede especificar otra carpeta.

  Los valores predeterminados para la opción de la línea de comandos `INSTALLDIR=<ruta completa a la carpeta>` son los siguientes:

  - Kaspersky Embedded Systems Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - Herramientas de administración: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
  - En la versión de 64 bits de Microsoft Windows: %ProgramFiles(x86)%

- La tarea de protección de archivos en tiempo real se inicia inmediatamente después de que se inicie Kaspersky Embedded Systems Security. Active esta configuración para iniciar la Protección de archivos en tiempo real al iniciar Kaspersky Embedded Systems Security (recomendado).

  Los valores posibles para la opción de la línea de comandos `RUNRTP=<valor>` son los siguientes:

  - `1` – iniciar (valor predeterminado).
  - `0`: no iniciar.

- Las exclusiones de la protección recomendadas por Microsoft Corporation. En la tarea Protección de archivos en tiempo real, excluya del alcance de la protección a los objetos del equipo que Microsoft Corporation recomiende excluir. Es posible que algunas aplicaciones instaladas en el equipo se vuelvan inestables si una aplicación antivirus intercepta o modifica los archivos utilizados. Por ejemplo, Microsoft Corporation incluye algunas aplicaciones del controlador de dominio en la lista de tales objetos.

  Los valores posibles para la opción de la línea de comandos `ADDMSEXCLUSION=<valor>` son los siguientes:

  - `1`: excluir (valor predeterminado).
  - `0`: no excluir.

- Los objetos excluidos del alcance de la protección según las recomendaciones de Kaspersky Lab. En la tarea Protección de archivos en tiempo real, excluya del alcance de la protección a los objetos del equipo que Kaspersky Lab recomiende excluir.

  Los valores posibles para la opción de la línea de comandos `ADDKLEXCLUSION=<valor>` son los siguientes:

  - `1`: excluir (valor predeterminado).
  - `0`: no excluir.

- Permite la conexión remota con la Consola de la aplicación. De forma predeterminada, no se permite la conexión remota para la Consola de la aplicación instalada en el equipo protegido. Durante la instalación, puede permitir la conexión. Kaspersky Embedded Systems Security crea reglas de autorización para el proceso kavfsgt.exe mediante la utilización del protocolo de TCP para todos los puertos.

  Los valores posibles para la opción de la línea de comandos `ALLOWREMOTECON=<valor>` son los siguientes:

  - `1`: permitir.
  - `0`: denegar (valor predeterminado).

- Ruta al archivo de clave. De forma predeterminada, Windows Installer buscar el archivo con la extensión .key en la carpeta \product del kit de distribución. Si la carpeta \product contiene varios archivos de clave,

Windows Installer seleccionará el que tenga la fecha de caducidad más alejada. Los archivos de clave pueden guardarse de antemano en la carpeta \product o especificando otra ruta con la opción de configuración **Agregar clave**. Para agregar una clave después de la instalación de Kaspersky Embedded Systems Security, utilice la herramienta administrativa que prefiera (por ejemplo, la Consola de la aplicación). Si no agrega una clave durante la instalación de la aplicación, Kaspersky Embedded Systems Security no funcionará.

- Ruta al archivo de configuración. Kaspersky Embedded Systems Security importa la configuración a partir del archivo de configuración especificado creado en la aplicación. Kaspersky Embedded Systems Security no importa contraseñas del archivo de configuración (por ejemplo, contraseñas de cuenta para iniciar tareas ni contraseñas para establecer conexión con un servidor proxy). Una vez que se hayan importado las configuraciones, deberá introducir todas las contraseñas de forma manual. Si no ha especificado ningún archivo de configuración, la aplicación empleará los valores predeterminados tras la instalación.

  No se especifica el valor predeterminado para `CONFIGPATH=<nombre del archivo de configuración>`.

- Cómo habilitar conexiones de red para la Consola de la aplicación. Use esta opción para instalar Kaspersky Embedded Systems Security en otro equipo. Puede administrar de forma remota la protección de un equipo desde otro equipo con la Consola de Kaspersky Embedded Systems Security instalada. El puerto 135 (TCP) se abre en el Firewall de Microsoft Windows, se permiten las conexiones de red del archivo ejecutable kavfsrcn.exe para la administración remota de Kaspersky Embedded Systems Security y se concede acceso a aplicaciones DCOM. Cuando finalice la instalación, agregue los usuarios al grupo de Administradores de ESS para permitirles administrar la aplicación de forma remota y autorice las conexiones de red para el servicio de Kaspersky Security Management (kavfsgt.exe file) en el equipo. Puede leer más sobre la configuración adicional cuando la Consola de Kaspersky Embedded Systems Security se instala en otro equipo (consulte la sección “Configuración avanzada después de instalar la Consola de la aplicación en otro equipo”, en la página 51).

  Los valores posibles para la opción de la línea de comandos `ADDWFEXCLUSION=<valor>` son los siguientes:

  - `1`: permitir.
  - `0`: denegar (valor predeterminado).

- Deshabilitación de la verificación de software incompatible. Utilice este parámetro para habilitar o deshabilitar la búsqueda de software incompatible durante la instalación en segundo plano de la aplicación en el equipo. Independientemente del valor de este parámetro, durante la instalación de Kaspersky Embedded Systems Security, la aplicación siempre advierte sobre otras versiones de la aplicación instalada en el equipo.

  Los valores posibles para la opción de la línea de comandos `SKIPINCOMPATIBLESW=<valor>` son los siguientes:

  - `0`: se realiza la verificación de software incompatible (valor predeterminado).
  - `1`: no se realiza la verificación de software incompatible.

Configuración de desinstalación y opciones de la línea de comandos en Windows Installer

- Restauración de objetos en cuarentena.

  Los valores posibles para la opción de la línea de comandos `RESTOREQTN=<valor>` son los siguientes:

  - `0`: eliminar el contenido puesto en cuarentena (valor predeterminado).
  - `1`: restaurar el contenido puesto en cuarentena en la carpeta especificada por el parámetro RESTOREPATH en la subcarpeta \Quarantine.

- Restauración del contenido de la copia de seguridad.

  Los valores posibles para la opción de la línea de comandos `RESTOREBCK=<valor>` son los siguientes:

  - `0`: eliminar el contenido de la copia de seguridad (valor predeterminado).
  - `1`: restaurar el contenido de la copia de seguridad en la carpeta especificada por el parámetro RESTOREPATH en la subcarpeta \Backup.
- Ingrese la contraseña actual para confirmar la desinstalación (si la protección con contraseña está habilitada).

  No se especifica el valor predeterminado para `UNLOCK_PASSWORD=<contraseña especificada>`.
- Carpeta de objetos restaurados. Los objetos restaurados se almacenan en la carpeta especificada.

  El valor predeterminado para la opción de la línea de comandos `RESTOREPATH=<ruta completa a la carpeta>` es %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored.

Registros de instalación y desinstalación de Kaspersky Embedded Systems Security

Si Kaspersky Embedded Systems Security se instala o desinstala con la ayuda del asistente de instalación (o desinstalación), el servicio Windows Installer crea un registro de instalación (o instalación). Un archivo de registro llamado ess_install_<uid>.log (donde <uid> es un identificador del registro único de 8 caracteres) se guardará en la carpeta %temp% para el usuario cuya cuenta se haya utilizado para iniciar el archivo setup.exe.

Si se ejecuta la opción **Modificar o eliminar las herramientas de administración de Kaspersky Embedded Systems Security 2.3** para la Consola de la aplicación o Kaspersky Embedded Systems Security en el menú **Iniciar**, se crea automáticamente un archivo de registro llamado ess_2.3_maintenance.log en la carpeta %temp%.

Si Kaspersky Embedded Systems Security se instala o desinstala desde la línea de comandos, el archivo de registro de instalación no se crea de manera predeterminada.

► *Para instalar Kaspersky Embedded Systems Security y crear un archivo de registro en el disco C:\:*

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

Planificación de la instalación

Esta sección describe el conjunto de herramientas de administración de Kaspersky Embedded Systems Security y aspectos especiales de la instalación y desinstalación de Kaspersky Embedded Systems Security con el asistente (consulte la sección “Instalación y desinstalación de la aplicación con el asistente”, en la página 47), desde la línea de comandos (consulte la sección “Instalación y desinstalación de la aplicación desde la línea de comandos”, en la página 60), mediante Kaspersky Security Center (consulte la sección “Instalación y desinstalación de la aplicación mediante Kaspersky Security Center”, en la página 65) y mediante directivas de grupos de Active Directory (consulte la sección “Instalación y desinstalación de la aplicación mediante directivas de grupos de Active

Directory” en la página 70).

Antes de iniciar la instalación Kaspersky Embedded Systems Security, planee las etapas principales de la instalación.

1. Defina qué herramientas de administración utilizará para configurar y administrar Kaspersky Embedded Systems Security.
2. Seleccione los componentes de la aplicación necesarios para la instalación (consulte la Sección "Códigos de componentes de software de Kaspersky Embedded Systems Security para el servicio de Windows Installer" en la página 33).
3. Elija el método de instalación.

En esta sección

Selección de herramientas de administración

Defina las herramientas de administración que utilizará para configurar Kaspersky Embedded Systems Security y para administrar la aplicación. Kaspersky Embedded Systems Security se puede administrar desde la Consola de la aplicación, la utilidad de línea de comandos y la Consola de administración de Kaspersky Security Center.

Consola de Kaspersky Embedded Systems Security

La Consola de Kaspersky Embedded Systems Security es un complemento independiente agregado a Microsoft Management Console. Kaspersky Embedded Systems Security se puede administrar mediante la Consola de la aplicación instalada en el equipo protegido o en cualquier otro equipo de la red corporativa.

Es posible agregar varios complementos de Kaspersky Embedded Systems Security a una Microsoft Management Console abierta en el modo de creación, a fin de usarla para administrar la protección de varios equipos en los que está instalado Kaspersky Embedded Systems Security.

La Consola de la aplicación se incluye en el conjunto de componentes de la aplicación “Herramientas de administración”.

Utilidad de línea de comandos

Puede administrar Kaspersky Embedded Systems Security desde la línea de comandos del equipo protegido.

La utilidad de línea de comandos está incluida en el grupo de componentes de la aplicación Kaspersky Embedded Systems Security.

Kaspersky Security Center

Si su empresa utiliza Kaspersky Security Center para administrar de forma centralizada la protección antivirus de los equipos, puede gestionar Kaspersky Embedded Systems Security a través de la Consola de administración de Kaspersky Security Center.

Deben instalarse los siguientes componentes:

- **Módulo de integración con el Agente de red de Kaspersky Security Center**. Este componente está incluido en el grupo de componentes de la aplicación Kaspersky Embedded Systems Security. Permite la

comunicación entre Kaspersky Embedded Systems Security y el Agente de red. Instale el módulo de integración con el Agente de red de Kaspersky Security Center en el equipo protegido.

- **Agente de red de Kaspersky Security Center**. Instale este componente en todos los equipos protegidos. Este componente admite la interacción entre la instancia de Kaspersky Embedded Systems Security instalada en el equipo y la Consola de administración de Kaspersky Security Center. El archivo de instalación del Agente de red se encuentra en la carpeta del kit de distribución de Kaspersky Security Center.
- **Complemento de administración de Kaspersky Embedded Systems Security 2.3**. Además, puede instalar el Complemento de administración para gestionar Kaspersky Embedded Systems Security a través de la Consola de administración en el equipo donde se instaló el servidor de administración de Kaspersky Security Center. Esto proporciona la interfaz para la administración de la aplicación mediante Kaspersky Security Center. El archivo de instalación del complemento de administración, \product\klcfginst.exe, está incluido en el kit de distribución de Kaspersky Embedded Systems Security.

Selección del tipo de instalación

Después de especificar los componentes de software para la instalación de Kaspersky Embedded Systems Security (consulte la sección “Códigos de componentes de software de Kaspersky Embedded Systems Security para el servicio de Windows Installer”, en la página 33), deberá seleccionar el método de instalación de la aplicación.

Seleccione el método de instalación en función de la arquitectura de la red y de las siguientes condiciones:

- Si necesita configuraciones de instalación de Kaspersky Embedded Systems Security especiales o la configuración de instalación recomendada (consulte la sección “Configuración de instalación y desinstalación y opciones de línea de comandos para el servicio de Windows Installer” en la página 40).
- Si la configuración de instalación será la misma para todos los equipos o específica para cada equipo.

Se puede instalar Kaspersky Embedded Systems Security de forma interactiva con el asistente de instalación o en modo silencioso sin la intervención del usuario, y se puede invocar mediante la ejecución del archivo del paquete de instalación con las opciones de instalación desde la línea de comandos. Puede instalar Kaspersky Embedded Systems Security de forma remota y centralizada mediante las políticas de grupo de Active Directory o ejecutando la tarea de instalación remota de Kaspersky Security Center.

Puede instalar y configurar Kaspersky Embedded Systems Security en un solo equipo y guardar sus valores de configuración en un archivo de configuración; en el futuro puede usar el archivo creado para instalar Kaspersky Embedded Systems Security en otros equipos. Tenga en cuenta que esta capacidad no existe cuando la aplicación se instala mediante las directivas del grupo de Active Directory.

Inicio del asistente de instalación

El asistente de instalación puede instalar los siguientes elementos:

- Componentes de Kaspersky Embedded Systems Security (consulte la sección “Componentes de software de Kaspersky Embedded Systems Security”, en la página 34) en un equipo protegido desde un archivo \product\setup.exe incluido en el kit de distribución.
- La Consola de Kaspersky Embedded Systems Security (consulte la sección “Instalación de la Consola de Kaspersky Embedded Systems Security” en la página 50) desde el archivo \console\setup.exe del kit de distribución en el equipo protegido u otro host LAN.

Ejecución del archivo del paquete de instalación desde la línea de comandos con la configuración de instalación requerida

Si el archivo del paquete de instalación se inicia sin opciones de línea de comandos, Kaspersky Embedded Systems Security se instalará con la configuración predeterminada. Las opciones de Kaspersky Embedded Systems Security pueden utilizarse para modificar la configuración de instalación.

La Consola de la aplicación puede instalarse en el equipo protegido o en la estación de trabajo del administrador.

También puede utilizar comandos de ejemplo para la instalación de Kaspersky Embedded Systems Security y la Consola de la aplicación (consulte la sección “Instalación y desinstalación de la aplicación desde la línea de comandos” en la página 60).

Instalación centralizada mediante Kaspersky Security Center

Si su red utiliza Kaspersky Security Center para administrar la protección antivirus de los equipos en red, Kaspersky Embedded Systems Security puede instalarse en varios equipos ejecutando la tarea de instalación remota.

Los equipos en los que quiera instalar Kaspersky Embedded Systems Security mediante Kaspersky Security Center (consulte la sección “Instalación y desinstalación de la aplicación mediante Kaspersky Security Center”, en la página 65) pueden encontrarse en el mismo dominio que Kaspersky Security Center, en otro dominio o no pertenecer a ninguno.

Instalación centralizada a partir de directivas de grupo de Active Directory

Las políticas de grupo de Active Directory pueden utilizarse para instalar Kaspersky Embedded Systems Security en un equipo protegido. La Consola de la aplicación puede instalarse en el equipo protegido o en la estación de trabajo del administrador.

Kaspersky Embedded Systems Security puede instalarse utilizando la configuración de instalación recomendada.

Los equipos en los cuales se instala Kaspersky Embedded Systems Security mediante directivas de grupo de Active Directory (consulte la sección “Instalación y desinstalación mediante directivas de grupo de Active Directory”, en la página 70) deben estar ubicados en el mismo dominio y en la misma unidad organizacional. La instalación se lleva a cabo al iniciar el equipo, antes de iniciar sesión en Microsoft Windows.

Instalación y desinstalación de la aplicación mediante un asistente

Esta sección describe la instalación y la desinstalación de Kaspersky Embedded Systems Security y de la Consola de la aplicación por medio del asistente de instalación, y contiene información sobre la configuración adicional de Kaspersky Embedded Systems Security y acciones a realizar después de la instalación.

En esta sección

Instalación mediante el asistente de instalación

Las siguientes secciones contienen información sobre la instalación de Kaspersky Embedded Systems Security y la Consola de la aplicación.

► *Para instalar y utilizar Kaspersky Embedded Systems Security, realice los siguientes pasos:*

1. Instale Kaspersky Embedded Systems Security en un equipo protegido.
2. Instale la Consola de la aplicación en los equipos desde los que administrará Kaspersky Embedded Systems Security.
3. Si la Consola de la aplicación se instaló en un equipo de la red, además de en el equipo protegido, deberá definir determinados parámetros de la configuración para permitir que los usuarios de la Consola de la aplicación administren Kaspersky Embedded Systems Security de forma remota.
4. Realice acciones después de la instalación de Kaspersky Embedded Systems Security.

En esta sección

Instalación de Kaspersky Embedded Systems Security

Antes de instalar Kaspersky Embedded Systems Security, realice los siguientes pasos:

Asegúrese de que no haya otros programas antivirus instalados en el equipo.

- Asegúrese de que la cuenta que utilizará para iniciar el asistente de instalación pertenezca al grupo de administradores del equipo protegido.

Después de completar las acciones descritas anteriormente, continúe con el procedimiento de instalación. Siga las indicaciones del asistente de instalación, especifique la configuración para la instalación de Kaspersky Embedded Systems Security. Puede detener el proceso de instalación de Kaspersky Embedded Systems Security en cualquier paso del asistente de instalación. Para ello, haga clic en el botón **Cancelar** que se encuentra en la ventana del asistente de instalación.

Puede leer más sobre la configuración de instalación (y desinstalación) (consulte la sección “Configuración de instalación y desinstalación y opciones de la línea de comandos para el servicio de Windows Installer”, en la página 40).

► *Para instalar Kaspersky Embedded Systems Security mediante el asistente de instalación:*

1. Inicie el archivo setup.exe en el equipo.
2. En la ventana que se abre, en la sección **Instalación**, haga clic en el vínculo **los términos y condiciones de este EULA**.
3. En la pantalla bienvenida del Asistente de instalación de Kaspersky Embedded Systems Security, haga clic en el botón **Siguiente**.

   Se abre la ventana **EULA y política de privacidad**.
4. Revise los términos del Contrato de licencia y la Política de privacidad.
5. Si acepta los términos y condiciones del Contrato de licencia de usuario final y la Política de privacidad, seleccione las casillas de los **los términos y condiciones de este EULA** y la **la Política de privacidad que describe el manejo de datos** a fin de continuar con la instalación.

   Si no acepta el Contrato de licencia de usuario final y/o la Política de privacidad, la instalación se cancelará.
6. Haga clic en el botón **Siguiente**.

   Se abrirá la ventana **Análisis rápido del equipo antes de la instalación**.
7. En la ventana **Análisis rápido del equipo antes de la instalación**, marque la casilla de verificación **Analizar el equipo en busca de virus** para buscar amenazas en la memoria del sistema o en los sectores de inicio de los discos del equipo local. Haga clic en el botón **Siguiente**. Una vez finalizado el procedimiento de análisis, el asistente abrirá una ventana con los resultados del análisis.

   Esta ventana tiene información acerca de los objetos analizados en el equipo: el número total de objetos analizados, el número de amenazas detectadas, el número de objetos infectados o probablemente infectados que se han detectado, el número de procesos peligrosos o sospechosos que Kaspersky Embedded Systems Security ha eliminado de la memoria y el número de procesos peligrosos o sospechosos que la aplicación no pudo eliminar.

   Para ver exactamente qué objetos se analizaron, pulse el botón **Lista de objetos procesados**.
8. Haga clic en el botón **Siguiente** en la ventana **Análisis rápido del equipo antes de la instalación**.

   Se abre la ventana **Instalación personalizada**.

9. Seleccione los componentes que quiera instalar.

   De forma predeterminada, todos los componentes de Kaspersky Embedded Systems Security se incluyen en el conjunto de instalación recomendado, excepto el componente de Administración del Firewall.

   > El componente Compatibilidad con Protocolo SNMP de Kaspersky Embedded Systems Security solo aparece en la lista de componentes que se sugiere instalar si el servicio Microsoft Windows SNMP está instalado en el equipo.

10. Para cancelar todos los cambios, haga clic en el botón **Restablecer** en la ventana **Instalación personalizada**. Haga clic en el botón **Siguiente**.
11. En la ventana **Seleccione una carpeta de destino**:
    - Si es necesario, especifique una carpeta en la cual se copiarán los archivos de Kaspersky Embedded Systems Security.
    - Si fuera necesario, revise la información sobre el espacio disponible en las unidades locales, haciendo clic en el botón **Disco**.

    Haga clic en el botón **Siguiente**.
12. En la ventana **Configuración avanzada de instalación**, configure las siguientes opciones de instalación:
    - **Habilitar la protección en tiempo real después de la instalación**.
    - **Agregar exclusiones recomendadas por Microsoft**.
    - **Agregar exclusiones recomendadas por Kaspersky Lab**.

      Haga clic en el botón **Siguiente**.
13. En la ventana **Importar opciones de configuración del archivo de configuración**:
    a. Especifique el archivo de configuración para importar Kaspersky Embedded Systems Security de un archivo de configuración existente creado en cualquier versión anterior de la aplicación.
    b. Haga clic en el botón **Siguiente**.
14. En la ventana **Activación de la aplicación**, realice una de las siguientes acciones:
    - Si desea activar la aplicación, especifique un archivo de clave de Kaspersky Embedded Systems Security.
    - Si desea activar la aplicación más adelante, haga clic en el botón **Siguiente**.
    - Si se ha guardado previamente un archivo de clave en la carpeta \product del kit de distribución, el nombre del archivo aparecerá en el campo **Clave**.

      > Para agregar una clave usando un archivo de clave guardado en otra carpeta, especifique el archivo.

      Una vez que se agrega el archivo de clave, la información sobre la licencia se mostrará en la ventana. Kaspersky Embedded Systems Security muestra la fecha de caducidad calculada de la licencia. El periodo de la licencia entra en vigor en el momento en que se agrega una clave y caduca antes de la fecha de caducidad del archivo de clave.

      Haga clic en el botón **Siguiente** para ingresar el archivo de clave en la aplicación.
15. En la ventana **Listo para instalar**, haga clic en el botón **Instalar**. El asistente comenzará con la instalación

de los componentes de Kaspersky Embedded Systems Security.

16. Una vez que termine la instalación, se abrirá la ventana **Instalación finalizada**.
17. Seleccione la casilla de verificación **Ver las Notas de la versión** para ver información sobre la versión después de que el asistente de instalación finalice.
18. Haga clic en **Finalizar**.

Se cierra el asistente de instalación. Una vez finalizada la instalación, ya podrá utilizar Kaspersky Embedded Systems Security si ha agregado la clave de activación.

Instalación de la Consola de Kaspersky Embedded Systems Security

Siga las instrucciones del asistente de instalación para configurar las opciones de instalación para la instalación de la Consola de la aplicación. Puede detener el proceso de instalación de Virus en cualquier paso del asistente de instalación. Para ello, haga clic en el botón **Cancelar** que se encuentra en la ventana del asistente de instalación.

► *Para instalar la Consola de la aplicación, siga estos pasos:*

1. Asegúrese de que la cuenta que utiliza para ejecutar el asistente de instalación pertenezca al grupo de administradores del equipo.
2. Ejecute el archivo setup.exe en el equipo.

   Se abre la ventana de bienvenida.
3. Haga clic en el vínculo **Instalar la consola de Kaspersky Embedded Systems Security**.

   Se abre la ventana de bienvenida del asistente de instalación.
4. Haga clic en el botón **Siguiente**.
5. Revise los términos del Contrato de licencia de usuario final en la ventana abierta y seleccione la casilla de verificación **Confirmo que he leído, entendido y que acepto los términos y las condiciones de este Contrato de licencia de usuario final** para continuar con la instalación.
6. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Configuración avanzada de instalación**.
7. En la ventana **Configuración avanzada de instalación**:
   - Si tiene pensado utilizar la Consola de la aplicación para administrar una instancia de Kaspersky Embedded Systems Security instalada en un equipo remoto, marque la casilla de verificación **Permitir el acceso remoto**.
   - Para abrir la **Instalación personalizada** y seleccionar componentes:
     a. Haga clic en el botón **Avanzado**.

        Se abre la ventana **Instalación personalizada**.
     b. Seleccione los componentes de las "Herramientas de administración" en la lista.

        De forma predeterminada, se instalan todos los componentes.
     c. Haga clic en el botón **Siguiente**.

> Puede encontrar más información sobre los componentes de Kaspersky Embedded Systems Security (consulte la sección “Códigos de componentes de software de Kaspersky Embedded Systems Security para el servicio de Windows Installer”, en la página 33).

8. En la ventana **Seleccione una carpeta de destino**:
   a. Si lo necesita, puede indicar otra carpeta en la que se guardarán los archivos de instalación.
   b. Haga clic en el botón **Siguiente**.
9. En la ventana **Listo para instalar**, haga clic en el botón **Instalar**.

   El asistente comenzará a instalar los componentes seleccionados.
10. Haga clic en **Finalizar**.

Se cierra el asistente de instalación. La Consola de la aplicación se instalará en el equipo protegido.

Si el conjunto de “Herramientas de administración” se instaló en un equipo de la red además del equipo protegido, ajuste la configuración avanzada (consulte la sección “Configuración avanzada después de la instalación de la Consola de la aplicación en otro equipo”, en la página 51).

Configuración avanzada después de la instalación de la Consola de la aplicación en otro equipo

Si la Consola de la aplicación se ha instalado en algún equipo en la red, además del equipo protegido, realice las siguientes acciones para que los usuarios pueden administrar Kaspersky Embedded Systems Security de forma remota:

- Agregar usuarios de Kaspersky Embedded Systems Security al grupo de administración de ESS en el equipo protegido.
- Permita conexiones de red para el servicio de Kaspersky Security Management (kavfsgt.exe) (consulte la sección “Acerca de los permisos para el servicio de Kaspersky Security Management”, en la página 224) si el equipo protegido utiliza el firewall de Windows u otro firewall.
- Si no se seleccionó la casilla **Permitir el acceso remoto** durante la instalación de la Consola de la aplicación en un equipo que ejecuta Microsoft Windows, permita manualmente conexiones de red para la Consola de la aplicación mediante el firewall del equipo.

La Consola de la aplicación en el equipo remoto utiliza el protocolo DCOM para recibir información sobre eventos de Kaspersky Embedded Systems Security (objetos analizados, tareas finalizadas, etc.) del servicio de Kaspersky Security Management en el equipo protegido. Debe permitir conexiones de red para la Consola de la aplicación en la configuración de Firewall de Windows para establecer conexiones entre la Consola de la aplicación y el servicio de Kaspersky Security Management.

En el equipo remoto, donde está instalada la Consola de la aplicación, haga lo siguiente:

- Asegúrese de que esté permitido el acceso remoto anónimo a las aplicaciones COM (pero no el inicio y la activación remotos de las aplicaciones COM).
- En el Firewall de Windows, abra el puerto TCP 135 y permita las conexiones de red para kavfsrcn.exe, el archivo ejecutable del proceso de administración remota de Kaspersky Embedded Systems Security.

  El equipo cliente en el que está instalada la Consola de la aplicación utiliza el puerto TCP 135 para acceder al equipo protegido y recibir una respuesta.
- Configure una regla saliente para el Firewall de Windows para permitir la conexión.

  A diferencia de los servicios de TCP/IP y UDP/IP tradicionales, donde un único protocolo tiene un puerto fijo, DCOM asigna dinámicamente puertos para los objetos COM remotos. Si existe un firewall entre el cliente (donde está instalada la Consola de la aplicación) y el terminal DCOM (el equipo protegido), debe abrirse un intervalo grande de puertos.

Los mismos pasos deben aplicarse para configurar cualquier otro firewall de software o hardware.

► *Si la consola de la aplicación está abierta mientras configura la conexión entre el equipo protegido y el equipo en el cual está instalada la consola de la aplicación:*

1. Cierre la consola de la aplicación.
2. Espere hasta que finalice el proceso de administración remota kavfsrcn.exe de Kaspersky Embedded Systems Security.
3. Reinicie la consola de la aplicación.

   Se aplicará la nueva configuración de conexión.

En esta sección

Permiso de acceso remoto anónimo a las aplicaciones COM

Los nombres de las opciones pueden variar según el sistema operativo Windows instalado.

► *Para permitir el acceso remoto anónimo a las aplicaciones COM, siga estos pasos:*

1. En el equipo remoto donde se encuentra instalada la Consola de Kaspersky Embedded Systems Security, abra la consola de Servicios de componentes.
2. Seleccione **Iniciar** → **Ejecutar**.
3. Escriba el comando `dcomcnfg`.
4. Haga clic en **Aceptar**.
5. Amplíe el nodo **Equipos** en la consola de **Servicios de componentes** en su equipo.
6. Abra el menú contextual en el nodo **Mi equipo**.
7. Seleccione **Propiedades**.
8. En la pestaña **Seguridad COM** de la ventana **Propiedades**, haga clic en el botón **Editar límites** ubicado en el grupo de opciones de configuración **Permisos de acceso**.
9. Asegúrese de que la casilla de verificación **Permitir el acceso remoto** esté activada para el usuario con INICIO DE SESIÓN ANÓNIMO en la ventana **Permitir el acceso remoto**.
10. Haga clic en **Aceptar**.

Permiso de conexión de red para el proceso de administración remota de Kaspersky Embedded Systems Security

Los nombres de las opciones pueden variar según el sistema operativo Windows instalado.

► *Para abrir el puerto TCP 135 en el firewall de Windows y permitir conexiones de red para el proceso de administración remota de Kaspersky Embedded Systems Security, siga los siguientes pasos:*

1. Cierre la Consola de Kaspersky Embedded Systems Security en el equipo remoto.
2. Realice uno de los siguientes pasos:
   - En Microsoft Windows XP SP2 o una versión posterior:
     a. Seleccione **Inicio** > **Firewall de Windows**.
     b. En la ventana **Firewall de Windows** (o Configuración de Firewall de Windows), haga clic en el botón **Agregar puerto** en la pestaña **Exclusiones**.
     c. En el campo **Nombre**, especifique el nombre del puerto RPC (TCP/135) o introduzca otro nombre, por ejemplo, DCOM de Kaspersky Embedded Systems Security, y especifique el número de puerto (135) en el campo **Nombre de puerto**.
     d. Seleccione el protocolo **TCP**.
     e. Haga clic en **Aceptar**.
     f. Presione el botón **Agregar** en la pestaña **Exclusiones**.
   - En Microsoft Windows 7 o una versión posterior:
     a. Seleccione **Iniciar** > **Panel de control** > **Firewall de Windows**.
     b. En la ventana **Firewall de Windows**, seleccione **Permitir un programa o una característica a través de Firewall de Windows**.
     c. En la ventana **Permitir que programas se comuniquen a través de Firewall de Windows**, haga clic en el botón **Permitir otro programa...**.
3. Especifique el archivo kavfsrcn.exe en la ventana **Agregar programa**. Está ubicado en la carpeta de destino especificada durante la instalación de la Consola de Kaspersky Embedded Systems Security mediante Microsoft Management Console.
4. Haga clic en **Aceptar**.
5. Haga clic en el botón **Aceptar** en la ventana Firewall de Windows (**Configuración de Firewall de Windows**).

Agregado de la regla saliente para el Firewall de Windows

Los nombres de las opciones pueden variar según el sistema operativo Windows instalado.

► *Para agregar la regla saliente para el Firewall de Windows, siga los siguientes pasos:*

1. Seleccione **Iniciar** > **Panel de control** > **Firewall de Windows**.
2. En la ventana **Firewall de Windows**, haga clic en el vínculo **Configuración avanzada**.

   Se abre la ventana **Firewall de Windows con seguridad avanzada**.
3. Seleccione el nodo secundario **Reglas salientes**.
4. Haga clic en la opción **Nueva regla** en el panel **Acciones**.
5. En la ventana **Nuevo asistente de regla saliente** que se abre, seleccione la opción **Puerto** y haga clic en **Siguiente**.
6. Seleccione el protocolo **TCP**.
7. En el campo **Puertos remotos específicos**, especifique el siguiente intervalo de puertos para permitir conexiones salientes: 1024-65535.
8. En la ventana **Acción**, seleccione la opción **Permitir la conexión**.
9. Guarde la nueva regla y cierre la ventana **Firewall de Windows con seguridad avanzada**.

Ahora el firewall de Windows permitirá conexiones de red entre la Consola de la aplicación y el servicio de Kaspersky Security Management.

Acciones para realizar después de la instalación de Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security inicia la protección y las tareas de análisis inmediatamente después de la instalación si ha activado la aplicación. Si se selecciona **Habilitar la protección en tiempo real después de la instalación** (opción predeterminada) durante la instalación de Kaspersky Embedded Systems Security, la aplicación analizará los objetos del sistema de archivos del equipo cuando acceda a ellos. Kaspersky Embedded Systems Security ejecutará la tarea Análisis de áreas críticas todos los viernes a las 20:00.

Le recomendamos realizar los siguientes pasos después de instalar Kaspersky Embedded Systems Security:

- Inicie la tarea de actualización de bases de datos de la aplicación. Después de la instalación, Kaspersky Embedded Systems Security analizará los objetos con la base de datos incluida en el kit de distribución de la aplicación.

  Recomendamos actualizar las bases de datos de Kaspersky Embedded Systems Security inmediatamente, ya que pueden estar desactualizadas.

  La aplicación actualizará la base de datos a cada hora, de acuerdo con la programación predeterminada de la tarea.
- Realice un análisis de áreas críticas del equipo si no había ningún software antivirus con protección de archivos en tiempo real instalado en el equipo protegido antes de la instalación de Kaspersky Embedded Systems Security.
- Configure las notificaciones del administrador sobre eventos de Kaspersky Embedded Systems Security.

En esta sección

Inicio y configuración de la tarea de Actualización de bases de datos de Kaspersky Embedded Systems Security

► *Para actualizar la base de datos de la aplicación después de la instalación, haga lo siguiente:*

1. En la configuración de la tarea Actualización de bases de datos, configure una conexión con el origen de actualizaciones a través de los servidores de actualizaciones FTP o HTTP de Kaspersky Lab.
2. Inicie la tarea Actualización de bases de datos.

El Protocolo de autodescubrimiento de Proxy Web (WPAD) no se puede configurar en su red para detectar la configuración del servidor proxy automáticamente en la red de área local. En eso, su red puede requerir la autenticación al acceder al servidor proxy.

► *Para especificar la configuración del servidor proxy opcional y la configuración de autenticación para acceder al servidor proxy, haga lo siguiente:*

1. Abra el menú contextual en el nodo **Kaspersky Embedded Systems Security**.
2. Seleccione el elemento **Propiedades**.

   Se abrirá la ventana **Configuración de la aplicación**.
3. Seleccione la pestaña **Configuración de conexión**.
4. En la sección **Configuración del servidor proxy**, seleccione la casilla **Usar la configuración especificada del servidor proxy**.
5. Ingrese la dirección del servidor proxy en el campo **Dirección** e ingrese el número de puerto para el servidor proxy en el campo **Puerto**.
6. En la sección **Configuración de autenticación del servidor proxy**, seleccione el método de autenticación necesario en la lista desplegable:
   - **Usar autenticación NTLM** si el servidor proxy admite la autenticación NTLM integrada en Microsoft Windows. Kaspersky Embedded Systems Security usará la cuenta de usuario especificada en las configuraciones de la tarea para acceder al servidor proxy (de forma predeterminada, la tarea se ejecuta con la cuenta de usuario **sistema local** [**SYSTEM**]).
   - **Usar autenticación NTLM con nombre de usuario y contraseña** si el servidor proxy admite la autenticación NTLM integrada en Microsoft Windows. Kaspersky Embedded Systems Security utilizará la cuenta especificada para acceder al servidor proxy. Introduzca un nombre de usuario y contraseña o seleccione un usuario de la lista.
   - **Aplicar nombre de usuario y contraseña** para seleccionar la autenticación básica. Introduzca un nombre de usuario y contraseña o seleccione un usuario de la lista.
7. Haga clic en **Aceptar** en la ventana **Configuración de la aplicación**.

► *Para configurar la conexión con los servidores de actualizaciones de Kaspersky Lab, en la tarea Actualización de bases de datos:*

1. Inicie la Consola de la aplicación de una de las siguientes maneras:
   - Abra la Consola de la aplicación en el equipo protegido. Para ello, seleccione **Iniciar** > **Todos los programas** > **Kaspersky Embedded Systems Security** > **Herramientas de administración** > **Consola de Kaspersky Embedded Systems Security 2.3**.
   - Si la Consola de la aplicación se ha iniciado en un equipo que no sea el protegido, conéctela al equipo protegido:
     a. Abra el menú contextual del nodo **Kaspersky Embedded Systems Security** en el árbol de la Consola de la aplicación.
     b. Seleccione el elemento **Conectarse a otro equipo**.
     c. En la ventana **Seleccionar equipo**, seleccione **Otro equipo** e indique el nombre de la red del equipo protegido en el campo de texto.

     Si la cuenta que usaba para iniciar sesión en Microsoft Windows no tiene permisos de acceso para el servicio de Kaspersky Security Management (consulte la sección “Acerca de los permisos de acceso al servicio de Kaspersky Security Management”, en la página 224), indique una cuenta que tenga estos permisos.

   Se abre la ventana Consola de la aplicación.
2. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
3. Seleccione el nodo secundario **Actualización de bases de datos**.
4. Haga clic en el vínculo **Propiedades** del panel de detalles.
5. En la ventana **Configuración de tareas** que se abre, abra la pestaña **Configuración de conexión**.
6. Seleccione **Usar servidor proxy para los servidores de actualizaciones de Kaspersky Lab**.
7. Haga clic en **Aceptar** en la ventana **Configuración de tareas**.

Se guardará la configuración para establecer conexión con el origen de actualizaciones en la tarea Actualización de bases de datos.

► *Para ejecutar la tarea de Actualización de bases de datos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
2. En el menú contextual del nodo secundario **Actualización de bases de datos**, seleccione el elemento **Iniciar**.

Iniciará la tarea Actualización de bases de datos.

Una vez que la tarea haya finalizado correctamente, podrá ver la fecha de lanzamiento de las últimas actualizaciones de bases de datos instaladas en el panel de detalles del nodo **Kaspersky Embedded Systems Security**.

Análisis de áreas críticas

Después de actualizar las bases de datos de Kaspersky Embedded Systems Security, analice el equipo en busca de malware con la tarea Análisis de áreas críticas.

► *Para ejecutar la tarea de análisis de áreas críticas, siga estos pasos:*

1. Expanda el nodo **Análisis a pedido** en el árbol de la Consola de la aplicación.
2. En el menú contextual del nodo secundario **Análisis de áreas críticas**, seleccione el comando **Iniciar**.

Cuando inicie la tarea, el panel de detalles mostrará el estado de tarea **En ejecución**.

► *Para ver el registro de tareas,*

en el panel de detalles del nodo **Análisis de áreas críticas**, haga clic en el vínculo **Abrir el registro de tareas**.

Modificación del conjunto de componentes y reparación de Kaspersky Embedded Systems Security

Puede agregar o quitar los componentes de Kaspersky Embedded Systems Security. Debe detener la tarea de Protección de archivos en tiempo real antes de poder eliminar el componente de Protección de archivos en tiempo real. En otros casos, no es necesario detener la protección de archivos en tiempo real ni el servicio de Kaspersky Security.

Si la administración de la aplicación está protegida con contraseña, Kaspersky Embedded Systems Security solicita la contraseña cuando intenta quitar componentes o modificar el conjunto de componentes en el asistente de instalación.

► *Para modificar el conjunto de componentes de Kaspersky Embedded Systems Security:*

1. En el menú **Iniciar**, seleccione **Todos los programas** > **Kaspersky Embedded Systems Security** > **Modificar o eliminar Kaspersky Embedded Systems Security**.

   Se abre la ventana **Modificar, reparar o eliminar la instalación** del asistente de instalación.
2. Seleccione **Modificar conjunto de componentes**. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Instalación personalizada**.
3. En la ventana de **Instalación personalizada**, en la lista de componentes disponibles, seleccione los componentes que desea agregar o quitar de Kaspersky Embedded Systems Security. Para ello, realice las siguientes acciones:

   - Para cambiar el conjunto de componentes, haga clic en el botón situado junto al nombre del componente seleccionado. Luego, en el menú contextual, seleccione:
     - **El componente se instalará en el disco duro local** si desea instalar un componente.
     - **El componente y sus subcomponentes se instalarán en el disco duro local** si desea instalar un grupo de componentes.
   - Para eliminar los componentes instalados previamente, haga clic en el botón situado junto al nombre del componente seleccionado. A continuación, en el menú contextual, seleccione **El componente no estará disponible**.

   Haga clic en el botón **Siguiente**.

4. En la ventana **Listo para instalar**, confirme los cambios en el conjunto de componentes haciendo clic en el botón **Instalar**.
5. Haga clic en el botón **Aceptar** en la ventana que se abre una vez completada la instalación.

El conjunto de componentes de Kaspersky Embedded Systems Security se modificará según la configuración especificada.

Si el funcionamiento de Kaspersky Embedded Systems Security presenta problemas (Kaspersky Embedded Systems Security deja de funcionar; las tareas dejan de funcionar o no se inician), puede intentar reparar Kaspersky Embedded Systems Security. Puede realizar una reparación y guardar la configuración actual de Kaspersky Embedded Systems Security, o puede seleccionar una opción para restablecer toda la configuración de Kaspersky Embedded Systems Security a sus valores predeterminados.

► *Para reparar Kaspersky Embedded Systems Security después de que la aplicación o una tarea deje de funcionar, realice los siguientes pasos:*

1. En el menú **Iniciar**, seleccione **Todos los programas**.
2. Seleccione **Kaspersky Embedded Systems Security**.
3. Seleccione **Modificar o eliminar Kaspersky Embedded Systems Security**.

   Se abre la ventana **Modificar, reparar o eliminar la instalación** del asistente de instalación.
4. Seleccione **Reparar componentes instalados**. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Reparar componentes instalados**.
5. En la ventana **Reparar componentes instalados**, seleccione la casilla de verificación **Restaurar la configuración recomendada de la aplicación** si desea restablecer las opciones de la aplicación y restaurar Kaspersky Embedded Systems Security con su configuración predeterminada. Haga clic en el botón **Siguiente**.
6. En la ventana **Listo para reparar**, confirme la operación de reparación haciendo clic en el botón **Instalar**.
7. Haga clic en el botón **Aceptar** en la ventana que se abre una vez completada la operación de reparación.

Kaspersky Embedded Systems Security se reparará utilizando la configuración especificada.

Desinstalación mediante el asistente de instalación

Esta sección contiene instrucciones sobre cómo desinstalar Kaspersky Embedded Systems Security y la Consola de la aplicación de un equipo protegido con el Asistente de instalación/desinstalación.

En esta sección

Desinstalación de Kaspersky Embedded Systems Security

Los nombres de configuración pueden variar en los diferentes sistemas operativos Windows.

Kaspersky Embedded Systems Security puede desinstalarse del equipo protegido con el asistente de instalación/desinstalación.

Después de la desinstalación de Kaspersky Embedded Systems Security de un equipo protegido, es posible que se requiera un reinicio. El reinicio se puede posponer.

Las opciones de desinstalación, reparación e instalación de la aplicación mediante el panel de control de Windows no están disponibles si el sistema operativo usa la función de UAC (Control de la cuenta de usuario) o el acceso a la aplicación está protegido por contraseña.

Si la administración de la aplicación está protegida con contraseña, Kaspersky Embedded Systems Security solicita la contraseña cuando intenta quitar componentes o modificar el conjunto de componentes en el asistente de instalación.

► *Para desinstalar Kaspersky Embedded Systems Security.*

1. En el menú **Iniciar**, seleccione **Todos los programas**.
2. Seleccione **Kaspersky Embedded Systems Security**.
3. Seleccione **Modificar o eliminar Kaspersky Embedded Systems Security**.

   Se abre la ventana **Modificar, reparar o eliminar la instalación** del asistente de instalación.
4. Seleccione **Eliminar componentes de software**. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Configuración avanzada de desinstalación de la aplicación**.
5. Si es necesario, en la ventana **Configuración avanzada de desinstalación de la aplicación**:
   a. Seleccione la casilla de verificación **Exportar objetos de Cuarentena** para exportar los objetos en cuarentena de Kaspersky Embedded Systems Security. De forma predeterminada, la casilla está desactivada.
   b. Seleccione la casilla de verificación **Exportar objetos de Copia de seguridad** para exportar los objetos de la copia de seguridad de Kaspersky Embedded Systems Security. De forma predeterminada, la casilla está desactivada.
   c. Haga clic en el botón **Guardar en** y seleccione la carpeta a la cual desea exportar los objetos. De forma predeterminada, los objetos se exportarán a %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall.

      Haga clic en el botón **Siguiente**.
6. En la ventana **Listo para desinstalar**, confirme la desinstalación haciendo clic en el botón **Desinstalar**.
7. Haga clic en el botón **Aceptar** en la ventana que se abre una vez completada la desinstalación.

Kaspersky Embedded Systems Security se desinstalará del equipo protegido.

Desinstalación de la Consola de Kaspersky Embedded Systems Security

Los nombres de configuración pueden variar en los diferentes sistemas operativos Windows.

Puede desinstalar la Consola de la aplicación del equipo con el asistente de instalación/desinstalación.

Después de desinstalar la Consola de la aplicación, no es necesario reiniciar el equipo.

► *Para desinstalar la Consola de la aplicación:*

1. En el menú **Iniciar**, seleccione **Todos los programas**.
2. Seleccione **Kaspersky Embedded Systems Security**.
3. Seleccione **Modificar o eliminar las herramientas de administración de Kaspersky Embedded Systems Security 2.3**.

   Se abrirá la ventana **Modificar, reparar o eliminar la instalación** del asistente.
4. Seleccione **Eliminar componentes de software** y haga clic en el botón **Siguiente**.
5. Se abre la ventana **Listo para desinstalar**. Haga clic en el botón **Desinstalar**.

   Se abre la ventana **Desinstalación finalizada**.
6. Haga clic en **Aceptar**.

Una vez que termine la desinstalación, la ventana del asistente de instalación se cerrará.

Instalación y desinstalación de la aplicación desde la línea de comandos

Esta sección indica cómo instalar y desinstalar Kaspersky Embedded Systems Security desde la línea de comandos y contiene ejemplos de comandos para realizar dichas acciones, así como ejemplos de comandos para agregar y quitar componentes de Kaspersky Embedded Systems Security desde la línea de comandos.

En esta sección

Acerca de la instalación y desinstalación de Kaspersky Embedded Systems Security desde la línea de comandos

Puede instalar o desinstalar Kaspersky Embedded Systems Security y agregar o quitar componentes al ejecutar los archivos del paquete de instalación llamado \product\ess_x86(x64).msi desde la línea de comandos después de haber especificado la configuración de instalación con claves.

El conjunto de "Herramientas de administración" puede instalarse en el equipo protegido o en otro equipo de la red y hacer que trabaje con la Consola de la aplicación de forma local o remota. Para ello, utilice el paquete de instalación \console\esstools.msi.

Lleve a cabo la instalación usando una cuenta incluida en el grupo de administradores del equipo en el que se instalará la aplicación.

Si ejecuta uno de los archivos \product\ess_x86.msi o \product\ess_x64.msi en el equipo protegido sin claves adicionales, Kaspersky Embedded Systems Security se instalará con la configuración de instalación recomendada.

Puede asignar el conjunto de componentes que se instalará con la opción de la línea de comandos ADDLOCAL; para ello, enumere los códigos de los componentes o conjuntos de componentes seleccionados.

Comandos de ejemplo para la instalación de Kaspersky Embedded Systems Security

Esta sección presenta ejemplos de comandos utilizados para instalar Kaspersky Embedded Systems Security.

En equipos con Microsoft Windows de 32 bits, ejecute los archivos con el sufijo x86 del kit de distribución. En equipos con Microsoft Windows de 64 bits, ejecute los archivos con el sufijo x64 del kit de distribución.

La información detallada sobre el uso de comandos estándares de Windows Installer y opciones de la línea de comandos se proporciona en la documentación suministrada por Microsoft.

Ejemplos de la instalación de Kaspersky Embedded Systems Security desde el archivo setup.exe

► *Para instalar Kaspersky Embedded Systems Security con la configuración de instalación recomendada sin intervención del usuario, ejecute el siguiente comando:*

```
\product\setup.exe /s/p EULA=1 PRIVACYPOLICY=1
```

Puede instalar Kaspersky Embedded Systems Security con la siguiente configuración:

- instalar solo los componentes Protección de archivos en tiempo real y Análisis a pedido;
- no ejecutar la función de protección de archivos en tiempo real al iniciar Kaspersky Embedded Systems Security;
- no excluir archivos que Microsoft Corporation recomienda excluir del alcance del análisis;

Para hacerlo, ejecute el siguiente comando:

```
\product\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

Ejemplos de comandos que se utilizan en la instalación: ejecutar un archivo .msi

- *Para instalar Kaspersky Embedded Systems Security con la configuración de instalación recomendada sin intervención del usuario, ejecute el siguiente comando:*

```
msiexec /i ess.msi /qn EULA=1 PRIVACYPOLICY=1
```

- *Para instalar Kaspersky Embedded Systems Security con la configuración de instalación recomendada y mostrar la interfaz de instalación, ejecute el siguiente comando:*

```
msiexec /i ess.msi /qf EULA=1 PRIVACYPOLICY=1
```

- *Para instalar y activar Kaspersky Embedded Systems Security utilizando el archivo de clave C:\0000000A.key:*

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1 PRIVACYPOLICY=1
```

- *Para instalar Kaspersky Embedded Systems Security con un análisis preliminar de los procesos activos y los sectores de inicio de los discos locales, ejecute el siguiente comando:*

```
msiexec /i ess.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

- *Para instalar Kaspersky Embedded Systems Security en la carpeta de instalación C:\ESS, ejecute el siguiente comando:*

```
msiexec /i ess.msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
```

- *Para instalar Kaspersky Embedded Systems Security y guardar un archivo de registro de instalación con el nombre ess.log en la carpeta donde se encuentra el archivo msi de Kaspersky Embedded Systems Security, ejecute el siguiente comando:*

```
msiexec /i ess.msi /l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
```

- *Para instalar la Consola de Kaspersky Embedded Systems Security, ejecute el siguiente comando:*

```
msiexec /i esstools.msi /qn EULA=1
```

- *Para instalar y activar Kaspersky Embedded Systems Security utilizando el archivo de clave C:\0000000A.key y configurar Kaspersky Embedded Systems Security según los ajustes del archivo de configuración C:\settings.xml, ejecute el siguiente comando:*

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key
CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

- *Para instalar un parche de la aplicación cuando Kaspersky Embedded Systems Security está protegido con contraseña, ejecute el siguiente comando:*

```
msiexec /p "<msp file name with path>" UNLOCK_PASSWORD=<password>
```

Acciones para realizar después de la instalación de Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security inicia la protección y las tareas de análisis inmediatamente después de la instalación si ha activado la aplicación. Si selecciona **Habilitar la protección en tiempo real después de la instalación** durante la instalación de Kaspersky Embedded Systems Security, la aplicación analizará los objetos del sistema de archivos del equipo cuando acceda a ellos. Kaspersky Embedded Systems Security ejecutará la tarea Análisis de áreas críticas todos los viernes a las 8:00 p. m.

Le recomendamos realizar los siguientes pasos después de instalar Kaspersky Embedded Systems Security:

- Inicie la tarea de actualización de bases de datos de Kaspersky Embedded Systems Security. Después de la instalación, Kaspersky Embedded Systems Security analizará los objetos con la base de datos incluida en el kit de distribución. Le recomendamos actualizar la base de datos de Kaspersky Embedded Systems Security de inmediato. Para ello, debe ejecutar la tarea de Actualización de bases de datos. La base de datos se actualizará cada hora de acuerdo con la programación predeterminada.

  Por ejemplo, puede ejecutar la tarea de Actualización de bases de datos de la aplicación con el siguiente comando:

  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456

  En este caso, las actualizaciones de bases de datos de Kaspersky Embedded Systems Security se descargan desde los servidores de actualizaciones de Kaspersky Lab. La conexión con el origen de actualizaciones se realiza a través de un servidor proxy (la dirección del servidor proxy es: proxy.company.com, puerto: 8080); para acceder al servidor, utilice la autenticación NTLM integrada en Windows y acceda con una cuenta (nombre de usuario: inetuser, contraseña: 123456).
- Realice un análisis de áreas críticas del equipo si no había ningún software antivirus con protección de archivos en tiempo real instalado en el equipo protegido antes de la instalación de Kaspersky Embedded Systems Security.

► *Para iniciar la tarea de Análisis de áreas críticas a través de la línea de comandos:*

KAVSHELL SCANCRITICAL /W:scancritical.log

Este comando guarda el registro de tareas en el archivo scancritical.log disponible en la carpeta actual.

- Configure las notificaciones del administrador sobre eventos de Kaspersky Embedded Systems Security.

Cómo agregar o eliminar componentes. Comandos de ejemplo

El componente Análisis a pedido se instala automáticamente. No es necesario especificarlo en la lista de valores clave de ADDLOCAL, agregando ni eliminando componentes de Kaspersky Embedded Systems Security.

► *Para agregar el componente Control de inicio de aplicaciones a los componentes que ya estén instalados, ejecute el siguiente comando:*

```
msiexec /i ess.msi ADDLOCAL=Oas,AppCtrl /qn
```

o

```
\product\setup.exe /s /p "ADDLOCAL=Oas,AppCtrl"
```

Si enumera los componentes que desea instalar junto con los componentes ya instalados, Kaspersky Embedded Systems Security instalará de nuevo los componentes existentes.

► *Para eliminar los componentes instalados, ejecute el siguiente comando:*

```
msiexec /i ess.msi
"ADDLOCAL=Oas,Ods,Ksn,AntiExploit,DevCtrl,Firewall,AntiCryptor,LogInspecto
r,AKIntegration,PerfMonCounters,SnmpSupport,Shell,TrayApp,AVProtection,Ram
Disk REMOVE=AppCtrl,Fim" /qn
```

Desinstalación de Kaspersky Embedded Systems Security. Comandos de ejemplo

► *Para desinstalar Kaspersky Embedded Systems Security desde el equipo protegido, ejecute el siguiente comando:*

```
msiexec /x ess.msi /qn
```

o

- Para sistemas operativos de 32 bits:

```
msiexec /x {51AACF7F-421E-40FA-B2B7-FCFE0BACF505} /qn
```

- Para sistemas operativos de 64 bits:

```
msiexec /x {673F3697-9D6C-4CF4-BB28-478492F45DDC} /qn
```

► *Para desinstalar la Consola de Kaspersky Embedded Systems Security, ejecute el siguiente comando:*

```
msiexec /x esstools.msi /qn
```

o

- Para sistemas operativos de 32 bits:

```
msiexec /x {26E7C356-E535-4434-9AB1-F1EA4E8A70F4} /qn
```

- Para sistemas operativos de 64 bits:

```
msiexec /x {7EC1A40D-52F4-4F8F-93BA-F6E68B152C26} /qn
```

► *Para desinstalar Kaspersky Embedded Systems Security de un equipo protegido donde esté habilitada la protección con contraseña, ejecute el siguiente comando:*

- Para sistemas operativos de 32 bits:

```
msiexec /x {51AACF7F-421E-40FA-B2B7-FCFE0BACF505} UNLOCK_PASSWORD=*** /qn
```

- Para sistemas operativos de 64 bits:

```
msiexec /x {673F3697-9D6C-4CF4-BB28-478492F45DDC} UNLOCK_PASSWORD=*** /qn
```

Códigos de devolución

La siguiente tabla contiene una lista de códigos de devolución de la línea de comandos.

Tabla 6. Códigos de devolución

Código	Descripción
1324	El nombre de la carpeta de destino contiene caracteres no válidos.
25001	Derechos insuficientes de instalar Kaspersky Embedded Systems Security. Para instalar la aplicación, inicie el asistente de instalación con derechos del administrador local.
25003	Kaspersky Embedded Systems Security no se puede instalar en equipos que ejecutan esta versión de Microsoft Windows. Inicie el asistente de instalación para versiones de 64 bits de Microsoft Windows.
25004	Se ha detectado un software incompatible. Para continuar la instalación, desinstale el siguiente software: <lista de softwares incompatibles>.
25010	La ruta indicada no se puede usar para guardar objetos puestos en cuarentena.
25011	El nombre de la carpeta para guardar objetos en cuarentena contiene caracteres no válidos.
26251	No es posible descargar DLL de contadores de rendimiento.
26252	No es posible descargar DLL de contadores de rendimiento.
27300	El controlador no se puede instalar.
27301	El controlador no se puede desinstalar.
27302	El componente de la red no se puede instalar. Se alcanzó la cantidad máxima admitida de dispositivos filtrados.
27303	Bases de datos antivirus no encontradas.

Instalación y desinstalación de la aplicación mediante Kaspersky Security Center

Esta sección contiene información general acerca de la instalación de Kaspersky Embedded Systems Security a través de Kaspersky Security Center. Asimismo, describe cómo instalar y desinstalar Kaspersky Embedded Systems Security mediante Kaspersky Security Center y otras tareas que deben realizarse tras la instalación de Kaspersky Embedded Systems Security.

En esta sección

Información general sobre la instalación mediante Kaspersky Security Center

Puede instalar Kaspersky Embedded Systems Security a través de Kaspersky Security Center ejecutando la tarea de instalación remota.

Una vez finalizada la tarea de instalación remota, Kaspersky Embedded Systems Security se instalará con la misma configuración en múltiples equipos.

Todos los equipos pueden combinarse en un solo grupo de administración y se puede crear una tarea de grupo que instale Kaspersky Embedded Systems Security en los equipos del grupo.

Puede crear una tarea que instale Kaspersky Embedded Systems Security de forma remota en un grupo de equipos que no pertenecen al mismo grupo de administración. Al crear esta tarea, debe generar una lista de los equipos individuales en los que se debe instalar Kaspersky Embedded Systems Security.

La información detallada acerca de la tarea de instalación remota está disponible en la *Ayuda de Kaspersky Security Center*.

Derechos para instalar o desinstalar Kaspersky Embedded Systems Security

La cuenta especificada en la tarea de instalación o desinstalación remota debe pertenecer al grupo de administradores en cada uno de los equipos protegidos en todos los casos, excepto en los descritos a continuación:

- Si el Agente de red de Kaspersky Security Center ya está instalado en los equipos en los que se instalará Kaspersky Embedded Systems Security (independientemente de en qué dominio estén los equipos o si pertenecen a alguno).

  > Si el Agente de red todavía no está instalado en los equipos, se puede instalar junto con Kaspersky Embedded Systems Security mediante una tarea de instalación remota. Antes de instalar el Agente de red, asegúrese de que la cuenta que indique en la tarea esté incluida en el grupo de administradores de cada uno de los equipos.

- Todos los equipos en los que desea instalar Kaspersky Embedded Systems Security pertenecen al mismo dominio como servidores de administración y el Servidor de administración está registrado como la cuenta **Administrador de dominio** (si esta cuenta dispone de derechos de administrador local en los equipos incluidos en el dominio).

De manera predeterminada, al usar el método **Instalación forzada**, la tarea de instalación remota se inicia desde la cuenta que ejecuta el servidor de administración.

Al trabajar con tareas de grupo o con tareas para grupos de equipos bajo el modo de instalación/desinstalación forzada, la cuenta debe disponer de los siguientes derechos en un equipo cliente:

- Derecho de ejecutar aplicaciones remotamente.
- Derechos sobre el recurso compartido **Admin$**.
- Derecho de **Iniciar sesión como servicio**.

Instalación de Kaspersky Embedded Systems Security a través de Kaspersky Security Center

La información detallada sobre la generación de un paquete de instalación y la creación de una tarea de instalación remota está disponible en la Guía de implementación de Kaspersky Security Center.

Si tiene pensado administrar Kaspersky Embedded Systems Security desde Kaspersky Security Center en el futuro, asegúrese de que se cumplan las siguientes condiciones:

- El equipo en el que está instalado el Servidor de administración de Kaspersky Security Center también tiene el Complemento de administración instalado (archivo \product\klcfginst.exe del kit de distribución de Kaspersky Embedded Systems Security).
- El Agente de red de Kaspersky Security Center está instalado en los equipos protegidos. Si el Agente de red de Kaspersky Security Center no está instalado en los equipos protegidos, puede instalarlo junto con Kaspersky Embedded Systems Security mediante una tarea de ejecución remota.

Los equipos también pueden combinarse en un grupo de administración para luego administrar la configuración de protección a través de las directivas y tareas de grupo de Kaspersky Security Center.

► *Para instalar Kaspersky Embedded Systems Security con la tarea de instalación remota:*

1. Inicie la Consola de administración de Kaspersky Security Center.
2. En Kaspersky Security Center, expanda el nodo **Avanzado**.
3. Expanda el nodo secundario **Instalación Remota**.
4. En el panel de detalles del nodo secundario **Paquetes de instalación**, haga clic en el botón **Crear paquete de instalación**.
5. Seleccione el tipo de paquete de instalación **Crear paquete de instalación para una aplicación de Kaspersky Lab**.
6. Ingrese el nombre del paquete de instalación.
7. Especifique el archivo ess.kud del kit de distribución de Kaspersky Embedded Systems Security como el archivo del paquete de instalación.

   Se abre la ventana **Contrato de licencia de usuario final y Política de privacidad**.
8. Si acepta los términos y condiciones del Contrato de licencia de usuario final y la Política de privacidad, seleccione las casillas de los **términos y condiciones de este Contrato de licencia de usuario final** y la **la Política de privacidad que describe el manejo de datos** a fin de continuar con la instalación.

   Debe aceptar el Contrato de licencia y la Política de privacidad para continuar.
9. Para cambiar el conjunto de componentes de Kaspersky Embedded Systems Security que se instalarán (consulte la sección “Modificación del conjunto de componentes y reparación de Kaspersky Embedded Systems Security”, en la página 57) y las opciones de instalación predeterminadas (consulte la sección “Configuración de instalación y desinstalación y opciones de la línea de comandos para el servicio de Windows Installer”, en la página 40) en el paquete de instalación:

   a. En Kaspersky Security Center, expanda el nodo **Instalación remota**.

   b. En el panel de detalles del nodo secundario **Paquetes de instalación**, abra el menú contextual del

paquete de instalación Kaspersky Embedded Systems Security creado y seleccione **Propiedades**.

c. En la ventana **Propiedades: <nombre del paquete de instalación>** ubicada en la sección **Configuración**, haga lo siguiente:

a. En el grupo de opciones de configuración **Componentes para instalar**, seleccione las casillas situadas junto a los nombres de los componentes de Kaspersky Embedded Systems Security que quiera instalar.

b. Para indicar una carpeta de destino que no sea la predeterminada, especifique el nombre y la ruta de la carpeta en el campo **Carpeta de destino**.

La ruta de acceso a la carpeta de destino puede contener variables de entorno del sistema. Si la carpeta no existe en el equipo, se creará.

c. En el grupo **Configuración avanzada de instalación**, configure los siguientes parámetros:

- **Analizar el equipo en busca de virus antes de la instalación**.
- **Habilitar la protección en tiempo real después de la instalación**.
- **Agregar exclusiones recomendadas por Microsoft a la lista de exclusiones**.

d. **Agregar exclusiones recomendadas por Kaspersky Lab a la lista de exclusiones**.

d. En la ventana **Propiedades: <nombre del paquete de instalación>**, haga clic en **Aceptar**.

10. En el nodo **Paquetes de instalación**, cree una tarea para instalar Kaspersky Embedded Systems Security de forma remota en los equipos seleccionados (grupo de administración). Configure los parámetros de la tarea.

Para saber más sobre la creación y configuración de tareas de instalación remotas, consulte la *Ayuda de Kaspersky Security Center*.

11. Ejecute la tarea de instalación remota de Kaspersky Embedded Systems Security.

Kaspersky Embedded Systems Security se instalará en los equipos especificados en la tarea.

Acciones para realizar después de la instalación de Kaspersky Embedded Systems Security

Después de instalar Kaspersky Embedded Systems Security, recomendamos que actualice las bases de datos de Kaspersky Embedded Systems Security en los equipos y realice un análisis de áreas críticas del equipo, en caso de que los equipos no hayan tenido instaladas aplicaciones antivirus con protección en tiempo real habilitada antes de la instalación de Kaspersky Embedded Systems Security.

Si los equipos en los que se instaló Kaspersky Embedded Systems Security forman parte del mismo grupo de administración en Kaspersky Security Center, puede llevar a cabo estas tareas de la siguiente manera:

1. Cree tareas de actualización de bases de datos para los grupos de equipos en los que se instaló Kaspersky Embedded Systems Security. Establezca el servidor de administración de Kaspersky Security Center como origen de actualizaciones.
2. Cree una tarea de grupo de Análisis a pedido con el estado del Análisis de áreas críticas. Kaspersky Security Center evalúa el estado de seguridad de cada uno de los equipos del grupo de acuerdo con los resultados de esta tarea, no en función de los resultados la tarea Análisis de áreas críticas.
3. Cree una directiva para el grupo de equipos. En las propiedades de la directiva, en la sección **Configuración de la aplicación**, desactive el inicio programado de las tareas de análisis a pedido del sistema y las tareas de Actualización de bases de datos en los equipos del grupo de administración en la

configuración de la subsección **Ejecutar tareas del sistema**.

También puede configurar las notificaciones del administrador sobre eventos de Kaspersky Embedded Systems Security.

Instalación de la Consola de la aplicación mediante Kaspersky Security Center

La información detallada sobre la creación de un paquete de instalación y la tarea de instalación remota está disponible en la Guía de implementación de Kaspersky Security Center.

► *Para instalar la Consola de la aplicación mediante una tarea de instalación:*

1. En la Consola de administración de Kaspersky Security Center, expanda el nodo **Avanzado**.
2. Expanda el nodo secundario **Instalación remota**.
3. En el panel de detalles del nodo secundario Paquetes de instalación, haga clic en el botón **Crear paquete de instalación**. Al crear el nuevo paquete de instalación:
   a. En la ventana **Asistente de paquete nuevo**, seleccione **Crear** un paquete de instalación para el archivo ejecutable especificado como un tipo de paquete.
   b. Ingrese el nombre del nuevo paquete de instalación.
   c. Seleccione el archivo \console\setup.exe de la carpeta del kit de distribución de Kaspersky Embedded Systems Security y seleccione la casilla de verificación **Copiar carpeta entera al paquete de instalación**.
   d. Si es necesario, use la opción de la línea de comandos ADDLOCAL para modificar el conjunto de componentes que desea instalar en el campo **Configuración de inicio del archivo ejecutable (opcional)** y cambie la carpeta de destino.

      Por ejemplo, para instalar únicamente la Consola de la aplicación en la carpeta C:\KasperskyConsole sin instalar el archivo de ayuda ni la documentación, use las siguientes opciones de línea de comandos:

      ```
      /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1"
      ```
4. En el nodo secundario **Paquetes de instalación**, cree una tarea para instalar la Consola de la aplicación de forma remota en los equipos seleccionados (grupo de administración). Configure los parámetros de la tarea.

   Para saber más sobre la creación y configuración de tareas de instalación remotas, consulte la ayuda de Kaspersky Security Center.
5. Ejecute la tarea de instalación remota.

La Consola de la aplicación se instalará en los equipos especificados en la tarea.

Desinstalación de Kaspersky Embedded Systems Security a través de Kaspersky Security Center

Si la administración de Kaspersky Embedded Systems Security en equipos de la red está protegida por contraseña, escriba la contraseña al crear una tarea para la desinstalación de varias aplicaciones. Si la protección por contraseña no está administrada centralmente por la directiva de Kaspersky Security Center, Kaspersky Embedded Systems Security se desinstalará correctamente desde los equipos protegidos en los cuales la contraseña introducida se corresponda con el valor establecido. Kaspersky Embedded Systems Security no se desinstalará de los otros equipos.

► *Para desinstalar Kaspersky Embedded Systems Security, siga los siguientes pasos en la Consola de administración de Kaspersky Security Center:*

1. En la Consola de administración de Kaspersky Security Center, cree e inicie una tarea de desinstalación de la aplicación.
2. En la tarea, seleccione el método de desinstalación (similar a la selección del método de instalación; consulte la sección anterior) y especifique la cuenta que el Servidor de administración usará para acceder a los equipos. Kaspersky Embedded Systems Security solo puede desinstalarse con la configuración de desinstalación predeterminada (consulte la sección “Configuración de instalación y desinstalación y opciones de la línea de comandos para el servicio de Windows Installer”, en la página 40).

Instalación y desinstalación a través de directivas de grupo de Active Directory

Esta sección describe cómo instalar y desinstalar Kaspersky Embedded Systems Security mediante políticas de grupo de Active Directory. También contiene información sobre las tareas a realizar tras la instalación de Kaspersky Embedded Systems Security a través de las políticas de grupo.

En esta sección

Instalación de Kaspersky Embedded Systems Security mediante directivas de grupo de Active Directory

Puede instalar Kaspersky Embedded Systems Security en varios equipos a través de la directiva de grupo de Active Directory. Puede instalar la Consola de la aplicación del mismo modo.

Los equipos donde desea instalar Kaspersky Embedded Systems Security o la Consola de la aplicación deben pertenecer al mismo dominio y a una sola unidad organizacional.

Los sistemas operativos de los equipos en los que desea instalar Kaspersky Embedded Systems Security utilizando la directiva deben tener la misma cantidad de bits (32 bits o 64 bits).

Usted debe disponer de derechos de administrador de dominio.

Para instalar Kaspersky Embedded Systems Security, use los paquetes de instalación de ess_x86(x64).msi. Para instalar la Consola de la aplicación, use los paquetes de instalación de esstools.msi.

Se ofrece información detallada sobre el uso de las directivas de grupo de Active Directory en la documentación provista por Microsoft.

► *Para instalar Kaspersky Embedded Systems Security (o la Consola de la aplicación):*

1. Guarde el archivo msi que corresponda a la cantidad de bits (32 bits o 64 bits) de la versión instalada del sistema operativo Microsoft Windows en la carpeta pública del controlador de dominio.
2. Guarde el archivo de clave (consulte la sección "Acerca del archivo clave" en la página 79) en la misma carpeta pública en el controlador de dominio.
3. En la misma carpeta pública en el controlador de dominio, cree un archivo install_props.json con los contenidos a continuación, los mismo especificarán que acepta las condiciones del Contrato de licencia y la Política de privacidad.

   ```
   {
   "EULA": "1",
   "PRIVACYPOLICY": "1"
   }
   ```

4. En el controlador de dominio, cree una nueva directiva para el grupo al que pertenezcan los equipos.
5. Utilice el **Editor de objetos de directiva de grupo** para crear un nuevo paquete de instalación en el nodo **Configuración del equipo**. Escriba la ruta del archivo msi de Kaspersky Embedded Systems Security (o la Consola de la aplicación) en el formato UNC (convención de nomenclatura universal).
6. Seleccione **Instalar siempre con privilegios elevados** en el servicio Windows Installer, tanto en el nodo **Configuración del equipo** como en el nodo **Configuración del usuario** del grupo seleccionado.
7. Aplique los cambios utilizando el comando `gpupdate / force`.

Kaspersky Embedded Systems Security se instalará en los equipos del grupo después de que se hayan reiniciado.

Acciones para realizar después de la instalación de Kaspersky Embedded Systems Security

Luego de instalar Kaspersky Embedded Systems Security en los equipos protegidos, se recomienda actualizar inmediatamente las bases de datos de la aplicación y ejecutar un Análisis de áreas críticas. Puede realizar estas acciones (consulte la sección “Acciones a realizar después de la instalación de Kaspersky Embedded Systems Security”, en la página 54) desde la Consola de la aplicación.

También puede configurar las notificaciones del administrador sobre eventos de Kaspersky Embedded Systems Security.

Desinstalación de Kaspersky Embedded Systems Security mediante políticas de grupo de Active Directory

Si utilizara una directiva del grupo de Active Directory para instalar Kaspersky Embedded Systems Security (o la Consola de la aplicación) en el grupo de equipos, puede utilizar esta directiva para desinstalar Kaspersky Embedded Systems Security (o la Consola de la aplicación).

La aplicación puede desinstalarse únicamente con los parámetros de desinstalación predeterminados.

Se ofrece información detallada sobre el uso de las directivas de grupo de Active Directory en la documentación provista por Microsoft.

Si la administración de la aplicación está protegida por contraseña, no puede desinstalar Kaspersky Embedded Systems Security utilizando directivas del grupo de Active Directory.

► *Para desinstalar Kaspersky Embedded Systems Security (o la Consola de la aplicación):*

1. En el controlador de dominio, seleccione la unidad organizativa desde cuyos equipos desea desinstalar Kaspersky Embedded Systems Security o la Consola de la aplicación.
2. Seleccione la directiva creada para la instalación de Kaspersky Embedded Systems Security, y en el **Editor de objetos de directivas de grupo**, en el nodo **Instalación de software** (**Configuración del equipo** > **Configuración de software** > **Instalación de software**), abra el menú contextual del paquete de instalación de Kaspersky Embedded Systems Security (o la Consola de la aplicación) y seleccione el comando **Todas las tareas > Eliminar**.
3. Seleccione el método de desinstalación **Desinstalar inmediatamente el software de usuarios y equipos**.
4. Aplique los cambios utilizando el comando `gpupdate / force`.

Kaspersky Embedded Systems Security se eliminará de los equipos después de que se hayan reiniciado y antes de iniciar sesión en Microsoft Windows.

Verificación de funciones de Kaspersky Embedded Systems Security. Uso del virus de prueba EICAR

Esta sección describe el virus de prueba EICAR y cómo debe utilizarse para verificar las funciones Protección en tiempo real y Análisis a pedido de Kaspersky Embedded Systems Security.

En esta sección

Acerca del virus de prueba EICAR

El virus de prueba fue diseñado para comprobar el funcionamiento de las aplicaciones antivirus. Fue desarrollado por el Instituto Europeo para la Investigación de los Antivirus Informáticos (EICAR).

El virus de prueba no es un objeto malicioso y no contiene código ejecutable para su equipo, aunque las aplicaciones antivirus de la mayoría de los proveedores lo detectan como una amenaza.

El archivo contiene el virus de prueba llamado eicar.com. Se puede descargar desde el sitio web de EICAR, http://www.eicar.org/anti_virus_test_file.htm.

Antes de guardar el archivo en una carpeta en el disco duro de su equipo, asegúrese de que la Protección de archivos en tiempo real esté deshabilitada en esa unidad.

El archivo eicar.com contiene una línea de texto. Al analizar el archivo, Kaspersky Embedded Systems Security detecta la amenaza de prueba en la línea de texto, le asigna el estado **Infectado** al archivo y lo elimina. La información acerca de la amenaza detectada en el archivo aparecerá en la Consola de la aplicación y en el registro de tareas.

Puede utilizar el archivo eicar.com para comprobar cómo Kaspersky Embedded Systems Security desinfecta los objetos infectados y cómo detecta objetos probablemente infectados. Para hacerlo, abra el archivo mediante un editor de texto, agregue uno de los prefijos enumerados en la tabla a continuación al principio de la línea de texto en el archivo y guarde el archivo con un nombre nuevo; por ejemplo, eicar_cure.com.

Para asegurarse de que Kaspersky Embedded Systems Security procese el archivo eicar.com con un prefijo, en la sección **Protección de objetos** de la configuración de seguridad, establezca el valor **Todos los objetos** en las tareas de Protección de archivos en tiempo real y Análisis a pedido de Kaspersky Embedded Systems Security.

Tabla 7. Prefijos de archivos EICAR

Prefijo	Estado del archivo después del análisis y la acción tomada por Kaspersky Embedded Systems Security
Sin prefijo	Kaspersky Embedded Systems Security le asigna el estado **Infectado** al objeto y lo elimina.
SUSP–	Kaspersky Embedded Systems Security le asigna el estado **Probablemente infectado** al objeto detectado por el analizador heurístico y lo elimina, ya que los objetos probablemente infectados no estén desinfectados.

Prefijo	Estado del archivo después del análisis y la acción tomada por Kaspersky Embedded Systems Security
Sin prefijo	Kaspersky Embedded Systems Security le asigna el estado **Infectado** al objeto y lo elimina.
WARN–	Kaspersky Embedded Systems Security le asigna el estado **Probablemente infectado** al objeto (el código del objeto coincide en parte con el código de una amenaza conocida) y lo elimina, ya que los objetos probablemente infectados no estén desinfectados.
CURE–	Kaspersky Embedded Systems Security le asigna el estado **Infectado** al objeto y lo desinfecta. Si la desinfección se realiza correctamente, la totalidad del texto del archivo se reemplaza con la palabra "CURE".

Verificación de las funciones Protección en tiempo real y Análisis a pedido

Después de instalar Kaspersky Embedded Systems Security, puede confirmarle a Kaspersky Embedded Systems Security que encuentre objetos que contengan código malicioso. Para comprobarlo, puede usar el virus de prueba de EICAR (consulte la sección “Acerca del virus de prueba EICAR”, en la página 73).

► *Para comprobar la función Protección en tiempo real, siga estos pasos:*

1. Descargue el archivo eicar.com en el sitio web de EICAR http://www.eicar.org/anti_virus_test_file.htm. Guárdelo en una carpeta pública en el disco local de cualquier equipo de la red.

   Antes de guardar el archivo en la carpeta, asegúrese de que la Protección de archivos en tiempo real esté deshabilitada para la carpeta.

2. Si desea comprobar que las notificaciones de red al usuario funcionen, asegúrese de que el servicio Windows Messenger de Microsoft esté habilitado tanto en el equipo protegido como en el equipo en el que guardó el archivo eicar.com.
3. Abra la Consola de la aplicación.
4. Copie el archivo eicar.com guardado en el disco local del equipo protegido mediante alguno de los siguientes métodos:
   - Para probar las notificaciones a través de una ventana Terminal Services, copie el archivo eicar.com en el equipo después de conectarlo al equipo mediante la utilidad Conexión remota a escritorio.
   - Para probar notificaciones a través del servicio Windows Messenger de Microsoft, use los sitios de la red del equipo para copiar el archivo eicar.com del equipo donde lo guardó.

La Protección de archivos en tiempo real funciona correctamente si se cumplen las siguientes condiciones:

- El archivo eicar.com se elimina del equipo protegido.
- En la Consola de la aplicación, se le asigna el estado *Crítico* al registro de tareas. El registro tiene una nueva línea con información sobre una amenaza en el archivo de eicar.com. (Para ver el registro de tareas, en el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**, seleccione la tarea **Protección de archivos en tiempo real** y finalmente, en el panel de información, haga clic en el vínculo **Abrir el registro de tareas**).

- Aparece el siguiente mensaje del servicio Windows Messenger de Microsoft en el equipo desde el que copió el archivo: `Kaspersky Embedded Systems Security bloqueó el acceso a <ruta del archivo en el equipo> \eicar.com en el equipo <nombre de red del equipo> a las <hora del evento>. Motivo: Amenaza detectada. Virus: EICAR-Test-File. Nombre de usuario: <nombre de usuario>. Nombre del equipo: <nombre de red del equipo desde el que se copió el archivo>`.

> Asegúrese de que el servicio Windows Messenger de Microsoft esté en ejecución en el equipo desde el que se copió el archivo eicar.com.

► *Para comprobar la función Análisis a pedido, siga estos pasos:*

1. Descargue el archivo eicar.com en el sitio web de EICAR http://www.eicar.org/anti_virus_test_file.htm. Guárdelo en una carpeta pública en el disco local de cualquier equipo de la red.

   > Antes de guardar el archivo en la carpeta, asegúrese de que la Protección de archivos en tiempo real esté deshabilitada para la carpeta.

2. Abra la Consola de la aplicación.
3. Haga lo siguiente:
   a. Expanda el nodo **Análisis a pedido** en el árbol de la Consola de la aplicación.
   b. Seleccione el nodo secundario **Análisis de áreas críticas**.
   c. En la pestaña **Configuración del área de análisis**, abra el menú contextual del nodo **Red** y seleccione **Agregar archivo de red**.
   d. Introduzca la ruta de acceso de red al archivo eicar.com en el equipo remoto con el formato UNC (convención de nomenclatura universal).
   e. Seleccione la casilla para incluir la ruta de acceso de red agregada en el área del análisis.
   f. Ejecute la tarea Análisis de áreas críticas.

El Análisis a pedido funciona correctamente si se cumplen las siguientes condiciones:

- El archivo eicar.com se elimina del disco duro del equipo.
- En la Consola de la aplicación, se le asigna el estado *Crítico* al registro de tareas. El registro de tareas del Análisis de áreas críticas tiene una nueva línea con información sobre una amenaza en el archivo eicar.com. (Para ver el registro de tareas, en el árbol de la Consola de la aplicación, expanda el nodo secundario **Análisis a pedido**, seleccione la tarea Análisis de áreas críticas y finalmente, en el panel de información, haga clic en el vínculo **Abrir el registro de tareas**).

Icono de interfaz de la aplicación

Puede controlar Kaspersky Embedded Systems Security mediante el Complemento de administración y la Consola de la aplicación local.

Las acciones en la interfaz Consola de la aplicación local se describen en la sección Cómo usar la Consola de la aplicación (consulte la sección "Cómo usar la Consola de Kaspersky Embedded Systems Security" en la página 134).

La interfaz de la Consola de administración de Kaspersky Security Center se usa para realizar acciones con el Complemento de administración. Consulte información detallada sobre la interfaz de Kaspersky Security Center en la *Ayuda de Kaspersky Security Center*.

Licencia de la aplicación

Esta sección brinda información sobre los conceptos principales relacionados con el otorgamiento de una licencia de la aplicación.

En este capítulo

Acerca del Contrato de licencia de usuario final

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

Recomendamos revisar detenidamente los términos del Contrato de licencia de usuario final antes de comenzar a usar la aplicación.

Puede revisar los términos del Contrato de licencia de usuario final de las siguientes formas:

- Durante la instalación de Kaspersky Embedded Systems Security
- Leyendo el archivo license.txt. Este documento está incluido en el kit de distribución de la aplicación.

Al confirmar que acepta el Contrato de licencia de usuario final al instalar la aplicación, debe indicar su aceptación de los términos del Contrato de licencia de usuario final. Si no acepta los términos del Contrato de licencia de usuario final, debe anular la instalación de la aplicación y no debe usarla.

Acerca de la licencia

Una licencia es un derecho con límite de tiempo para usar la aplicación que se le otorga de acuerdo con el Contrato de licencia de usuario final.

Una licencia válida le da derecho a recibir los siguientes servicios:

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

El área de servicio y el periodo de uso de la aplicación dependen del tipo de licencia que se utilizó para activar la aplicación.

La aplicación se activa usando un archivo de clave o un código de activación para una licencia comercial comprada.

Una licencia comercial es una licencia paga otorgada con la compra de la aplicación.

Kaspersky Embedded Systems Security implica las siguientes licencias comerciales:

- Licencia estándar de Kaspersky Embedded Systems Security.
- Licencia extendida de Kaspersky Embedded Systems Security Compliance Edition, que incluye dos componentes de inspección adicionales del sistema: Monitor de integridad de archivos e inspección de registros.

Cuando expira una licencia comercial, la aplicación sigue ejecutándose, pero algunas de sus funciones dejan de estar disponibles (por ejemplo, las bases de datos de Kaspersky Embedded Systems Security no se pueden actualizar). Para seguir usando todas las funciones de Kaspersky Embedded Systems Security, debe renovar su licencia comercial.

Para garantizar la máxima protección de su equipo contra amenazas a la seguridad, recomendamos renovar la licencia antes de que expire.

Asegúrese de que la clave adicional que agrega tenga una fecha de caducidad posterior que la activa.

Acerca del certificado de licencia

Un *certificado de licencia* es un documento que se le entrega junto con un archivo de clave o un código de activación (si corresponde).

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

- Número de pedido
- Información acerca del usuario a quien se le ha otorgado la licencia
- Información acerca de la aplicación que puede activarse con la licencia proporcionada
- Límite del número de unidades de licencia (es decir, dispositivos en los cuales puede usarse la aplicación con la licencia proporcionada)
- Fecha de inicio de validez de la licencia
- Fecha de caducidad de la licencia o término de la licencia
- Tipo de licencia

Acerca de la clave

Una *clave* es una secuencia de bits con la cual puede activar y posteriormente usar la aplicación de acuerdo con los términos del Contrato de licencia de usuario final. Kaspersky Lab genera una clave.

Para agregar una clave a la aplicación, use un archivo de clave. Luego de agregar una clave a la aplicación, esta aparece en la interfaz de la aplicación como una secuencia alfanumérica exclusiva.

Kaspersky Lab puede incluir una clave en una lista negra si se producen infracciones del Contrato de licencia. Si se bloquea su clave, se debe agregar una clave diferente para que funcione la aplicación.

Una clave puede ser una "clave activa" o una "clave adicional".

Una *clave activa* es la clave que usa la aplicación actualmente para funcionar. Se puede agregar una clave para una licencia comercial o de prueba como clave activa. La aplicación no puede tener más de una clave activa.

Una *clave adicional* es una clave que confirma el derecho de usar la aplicación pero que actualmente no se encuentra en uso. La clave adicional se activa automáticamente cuando expira la licencia asociada con la clave actual activa. Se puede agregar una clave adicional solo si hay una clave activa.

Acerca del archivo de clave

Un *archivo de clave* es un archivo con la extensión .key provisto por Kaspersky Lab. Los archivos de clave están diseñados para activar la aplicación mediante la adición de una clave de licencia.

Usted recibe un archivo de clave en la dirección de correo electrónico que proporcionó cuando compró Kaspersky Embedded Systems Security o cuando solicitó la versión de prueba de Kaspersky Embedded Systems Security.

No necesita conectarse con los servidores de activación de Kaspersky Lab para activar la aplicación con un archivo de clave.

Puede restaurar un archivo de clave si lo ha eliminado accidentalmente. Es posible que necesite un archivo de clave para registrar Kaspersky CompanyAccount, por ejemplo.

Para restaurar su archivo de clave, realice una de las siguientes acciones:

- Contacte al vendedor de la licencia.
- Reciba un archivo de clave a través del sitio web de Kaspersky Lab (https://keyfile.kaspersky.com/sp/) usando su código de activación disponible.

Acerca del código de activación

Un *código de activación* es una secuencia única de 20 letras y números. Debe introducir un código de activación para poder agregar una clave de activación de Kaspersky Embedded Systems Security. Recibirá el código de activación en la dirección de correo electrónico que proporcionó al comprar Kaspersky Embedded Systems Security.

Para activar la aplicación con un código de activación, necesita acceso a Internet a fin de conectarse con los servidores de activación de Kaspersky Lab.

Si ha perdido su código de activación después de instalar la aplicación, puede recuperarlo. Es posible que necesite el código de activación para registrar Kaspersky CompanyAccount, por ejemplo. Para recuperar su código de activación, póngase en contacto con el Servicio de soporte técnico de Kaspersky Lab.

Sobre la provisión de datos

El Contrato de licencia para Kaspersky Embedded Systems Security, específicamente la sección titulada "Términos del procesamiento de datos", especifica los términos, la responsabilidad legal y el procedimiento para enviar y procesar los datos indicados en esta Guía. Antes de aceptar el Contrato de licencia, revise detenidamente sus términos, además de todos los documentos vinculados con el Contrato de licencia.

Los datos que Kaspersky Lab recibe cuando usted utiliza la aplicación se protegen y se procesan de acuerdo con la Política de privacidad, disponible en www.kaspersky.com/Products-and-Services-Privacy-Policy.

Al aceptar los términos del Contrato de licencia, acepta enviar automáticamente los siguientes datos a Kaspersky Lab:

- Admitir el mecanismo para recibir actualizaciones; información sobre la aplicación instalada y su activación: el identificador de la aplicación instalada y su versión completa, incluido el número de compilación, el tipo, y el identificador de licencia, el identificador de instalación y el identificador de tarea de actualización.
- Usar la capacidad de explorar artículos de la Base de conocimientos cuando se produzcan errores en la aplicación (servicio de Redirección); información sobre la aplicación y el tipo del vínculo, específicamente: el nombre, la configuración regional y el número de versión completo de la aplicación, el tipo de vínculo de redirección y el identificador del error.
- Administrar confirmaciones para el procesamiento de datos; información sobre el estado de aceptación de contratos de licencia y otros documentos que estipulan términos de transferencia de datos: el identificador y la versión del Contrato de licencia u otro documento, como parte de los cuales se aceptan o se rechazan los términos de procesamiento de datos; un atributo, indicando la acción del usuario (confirmación o retiro de la aceptación de los términos); la fecha y la hora de los cambios de estado de la aceptación de los términos de procesamiento de datos.

Puede revisar los términos del Contrato de licencia de usuario final de las siguientes formas:

- Durante la instalación de la aplicación Kaspersky Embedded Systems Security, el asistente de instalación muestra el texto completo del Contrato de licencia en un paso donde se requiere la aceptación de sus términos.
- En cualquier momento en el archivo .TXT (license.txt), que contiene el texto completo del Contrato de licencia. El archivo se incluye en el kit de distribución de Kaspersky Embedded Systems Security, junto con los archivos de instalación de la aplicación.

Procesamiento de datos local

Al ejecutar las funciones principales de la aplicación descritas en esta Guía, Kaspersky Embedded Systems Security procesa y almacena localmente una secuencia de tipos de datos en el equipo protegido. Los datos que la aplicación procesa localmente no se envían automáticamente a Kaspersky Lab ni a otros sistemas de terceros.

Kaspersky Embedded Systems Security procesa y almacena localmente los siguientes datos:

- Información sobre archivos analizados y objetos detectados; por ejemplo, nombres y atributos de archivos procesados y rutas completas de los archivos en los medios analizados, tipos de archivos, acciones realizadas en archivos analizados, cuentas de usuarios que realizan cualquier acción en la red protegida o el equipo protegido, nombres y datos de los dispositivos analizados, información sobre procesos que se ejecutan en el sistema, sumas de control (MD5, SHA-256), marcas de fecha y hora, atributos del certificado digital, datos sobre los scripts ejecutados.
- Información sobre la actividad y la configuración del sistema operativo, por ejemplo, la configuración del Firewall de Windows, entradas del registro de eventos de Windows, nombres de cuentas de usuario, inicios de archivos ejecutables, sus sumas de control y atributos.

Kaspersky Embedded Systems Security procesa y almacena datos como parte de la funcionalidad básica de la aplicación, especialmente para registrar eventos de aplicaciones y recibir datos de diagnóstico. Los datos procesados localmente están protegidos según las opciones configuradas y aplicadas.

Kaspersky Embedded Systems Security le permite configurar el nivel de la protección para los datos procesados localmente: puede cambiar los privilegios del usuario para acceder a datos de proceso, cambiar periodos de retención para tales datos, deshabilitar de manera parcial o total la funcionalidad que involucra el registro de datos, y cambiar la ruta y los atributos de la carpeta donde se registran los datos.

La información detallada sobre la configuración de la funcionalidad de la aplicación que involucra el procesamiento de la información y la configuración predeterminada de almacenamiento de los datos procesados puede encontrarse en las secciones correspondientes de esta Guía.

De forma predeterminada, todos los datos que la aplicación procesa localmente durante la operación se eliminan después de la eliminación de Kaspersky Embedded Systems Security del equipo.

La excepción se aplica a los archivos con información de diagnóstico (archivos de rastreo y volcado) y los eventos de la aplicación en el registro de eventos de Windows: se recomienda eliminar estos archivos manualmente.

Puede encontrar información detallada sobre cómo trabajar con archivos que contienen datos de diagnóstico de la aplicación en las secciones correspondientes de esta Guía.

Puede eliminar los archivos de registro de eventos de Windows que contienen los eventos del programa de Kaspersky Embedded Systems Security a través de los medios estándar del sistema operativo.

Procesamiento local de datos mediante la aplicación de componentes auxiliares.

El paquete de instalación de Kaspersky Embedded Systems Security comprende los componentes auxiliares de la aplicación, que se pueden instalar en su servidor o equipo, incluso si Kaspersky Embedded Systems Security no está instalado en él. Los componentes auxiliares son los siguientes:

- Consola de la aplicación. Este componente se incluye en el conjunto de herramientas de administración de Kaspersky Embedded Systems Security y está representado por un complemento de Microsoft Management Console.
- El complemento de administración. Este componente proporciona una integración completa con la aplicación de Kaspersky Security Center.

Al realizar las funciones principales de la aplicación que se detallan en esta Guía, los componentes auxiliares de la aplicación procesan y almacenan localmente un conjunto de datos en el equipo donde están instalados, incluso si se instalan por separado de Kaspersky Embedded Systems Security.

Los componentes de la aplicación procesan y almacenan localmente los siguientes datos:

- La consola de la aplicación: el nombre del equipo que tiene instalado Kaspersky Embedded Systems Security (dirección IP o nombre de dominio) al que se conectó por última vez la consola de la aplicación; muestra los parámetros configurados en el complemento de Microsoft Management Console; datos sobre la última carpeta en la que el usuario seleccionó objetos a través de la consola de la aplicación (mediante el cuadro de diálogo del sistema que se abre al hacer clic en el botón **Examinar**). Los archivos de seguimiento de la consola de la aplicación también pueden contener los siguientes datos: el nombre del equipo que tiene instalada la aplicación Kaspersky Embedded Systems Security con la que se estableció la conexión remota, el nombre de la cuenta de usuario con la que se estableció la conexión remota.
- El complemento de administración puede procesar y almacenar temporalmente los datos procesados por Kaspersky Embedded Systems Security; por ejemplo, parámetros configurados de las tareas y de los componentes de la aplicación, parámetros de las políticas de Kaspersky Security Center, datos enviados en las listas de la red.

Los datos que los componentes auxiliares procesan no se envían automáticamente a Kaspersky Lab ni a otros

sistemas de terceros.

De forma predeterminada, todos los datos que los componentes auxiliares de la aplicación procesan localmente durante la operación se eliminan después de la eliminación de estos componentes.

Las excepciones son los archivos de rastreo de los componentes auxiliares de la aplicación, se recomienda eliminar estos archivos manualmente.

Puede encontrar información detallada sobre cómo trabajar con archivos que contienen datos de diagnóstico de los componentes auxiliares de la aplicación en las secciones correspondientes de esta Guía.

Activación de aplicación con una clave de licencia

Puede activar Kaspersky Embedded Systems Security al aplicar un archivo de clave.

Si ya se ha agregado una clave activa a Kaspersky Embedded Systems Security y se agrega otra clave como clave activa, la nueva clave sustituye a la clave agregada previamente. La clave agregada previamente se elimina.

Si ya se ha agregado una clave adicional a Kaspersky Embedded Systems Security y se agrega otra clave como clave adicional, la nueva clave sustituye a la clave agregada previamente. La clave adicional agregada previamente se elimina.

Si ya se han agregado una clave activa y una clave adicional a Kaspersky Embedded Systems Security y se agrega una nueva clave como clave activa, la nueva clave sustituye a la clave activa agregada anteriormente y la clave adicional no se elimina.

► *Para activar Kaspersky Embedded Systems Security con el archivo de clave, realice los siguientes pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Licencia**.
2. En el panel de detalles del nodo **Licencia**, haga clic en el vínculo **Agregar clave**.
3. En la ventana que se abre, haga clic en el botón **Examinar** y seleccione un archivo de clave con la extensión .key.

   También puede agregar una clave como clave adicional. Para agregar una clave como clave adicional, seleccione la casilla de verificación **Usar como clave adicional**.

4. Haga clic en **Aceptar**.

Se aplicará el archivo de clave seleccionado. La información sobre la clave agregada estará disponible en el nodo **Licencia**.

Activación de la aplicación con un código de activación

Para activar la aplicación utilizando un código de activación, el equipo debe estar conectado a Internet.

Puede activar Kaspersky Embedded Systems Security mediante un código de activación.

Al activar la aplicación con este método, Kaspersky Embedded Systems Security envía datos al servidor de activación para verificar el código ingresado:

- Si la verificación del código de activación es exitosa, la aplicación se activa.
- Si la verificación del código de activación falla, aparece la notificación correspondiente. En este caso, debe comunicarse con el proveedor de software al que compró su licencia de Kaspersky Embedded Systems Security.
- Si se excede la cantidad de activaciones con el código de activación, aparece la notificación correspondiente. El procedimiento de activación de la aplicación se interrumpe, y la aplicación le sugiere ponerse en contacto con el Servicio de soporte técnico de Kaspersky Lab.

► *Para obtener una clave para activar Kaspersky Embedded Systems Security usando un código de activación, siga los siguientes pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Licencia**.
2. En el panel de detalles del nodo **Licencia**, haga clic en el vínculo **Agregar código de activación**.
3. En la ventana que se abre, ingrese el código de activación en el campo **Código de activación**.
   - Si desea utilizar el código de activación como una clave adicional, active la casilla de verificación **Usar como clave adicional**.
   - Si desea ver la información de la licencia, haga clic en el botón **Ver información de licencia** que se mostrará en el cuadro de grupo la **Información sobre la licencia**.
4. Haga clic en **Aceptar**.

   Kaspersky Embedded Systems Security envía información sobre el código de activación que se ingresó al servidor de activación.

Visualización de información de la licencia actual

Visualización de información de la licencia

La información sobre la licencia actual se muestra en el panel de detalles del nodo **Kaspersky Embedded Systems Security** de la Consola de la aplicación. Una clave puede tener los siguientes estados:

- **Verificando el estado de la clave**: Kaspersky Embedded Systems Security está comprobando el archivo de clave o código de activación aplicado y espera una respuesta sobre el estado de la clave actual.
- **Fecha de caducidad de la licencia**: Kaspersky Embedded Systems Security se ha activado hasta la fecha y la hora especificadas. El estado de la clave se resalta en amarillo en los siguientes casos:
  - La licencia caducará en 14 días, y no se aplicó ninguna clave adicional.
  - La clave agregada se ha colocado en una lista negra y se bloqueará.
- **La licencia ha caducado**: Kaspersky Embedded Systems Security no se activa porque la licencia ha caducado. El estado se resalta en rojo.
- **Infracción del Contrato de licencia de usuario final**: Kaspersky Embedded Systems Security no se activa porque se han infringido los términos del Contrato de licencia de usuario final (consulte la sección “Acerca del Contrato de licencia de usuario final” en la página 77). El estado se resalta en rojo.
- **La clave está en la lista negra**: la clave agregada se ha bloqueado y Kaspersky Lab la ha puesto en una lista negra, por ejemplo, en el caso de que terceros utilicen la clave para activar la aplicación ilegalmente.

El estado se resalta en rojo.

Visualización de información acerca de la licencia actual

► *Para visualizar la información acerca de la licencia actual,*

en el árbol de la Consola de la aplicación, expanda el nodo **Licencia**.

La información general acerca de la licencia actual se muestra en el panel de detalles del nodo **Licencia** (consulte la tabla a continuación).

Tabla 8. Información general acerca de la licencia en el nodo Licencia

Campo	Descripción
Código de activación	El código de activación. Este campo se completa si activa la aplicación con un código de activación.
Estado de activación	Información sobre el estado de la activación de la aplicación. La columna **Activación** del panel de detalles del nodo **Licencia** puede tener los siguientes estados: • **Aplicada**: si ha activado la aplicación con un código de activación o archivo de clave. **Activación**: si ha aplicado un código de activación para activar la aplicación, pero el proceso de activación aún no ha finalizado. Se han completado los cambios de estado a *Aplicado* después de la activación de la aplicación y se han actualizado los contenidos del panel de detalles del nodo. • **Error de activación**: si se produjo un error en la activación de la aplicación. Puede ver la causa del error en la activación en el registro de tareas.
Clave	La clave utilizada para activar la aplicación.
Tipo de licencia	Tipo de licencia: comercial o de prueba.
Fecha de caducidad	La fecha y hora de caducidad de la licencia asociada con la clave activa.
Estado del código de activación o estado de la clave	Estado del código de activación o estado de la clave: Activo o adicional.

► *Para obtener información detallada acerca de la licencia,*

en el nodo **Licencia**, abra el menú contextual en la línea con los datos de la licencia que desea ampliar y seleccione **Propiedades**.

En la ventana **Propiedades:** En la pestaña **General** de la ventana **<Estado del código de activación o estado de la clave>**, se muestra información detallada acerca de la licencia actual y, en la pestaña **Avanzado**, está disponible información sobre el cliente e información de contacto de Kaspersky Lab o el distribuidor donde compró Kaspersky Embedded Systems Security (consulte la tabla a continuación).

Tabla 9. Información detallada de la licencia en la ventana Propiedades: <estado del código de activación o estado de la clave>

Campo	Descripción
Ficha General	
Clave	La clave utilizada para activar la aplicación.

Campo	Descripción
Fecha de adición de clave	Fecha en la que se agregó la clave a la aplicación.
Tipo de licencia	Tipo de licencia: comercial o de prueba.
Días hasta la fecha de caducidad	Cantidad de días restantes hasta la caducidad de la licencia asociada con la clave activa.
Fecha de caducidad	La fecha y hora de caducidad de la licencia asociada con la clave activa. Si activa la aplicación con una suscripción ilimitada, el valor del campo es *Ilimitada*. Si Kaspersky Embedded Systems Security no puede determinar la fecha de caducidad de la licencia, el valor del campo es *Desconocido*.
Aplicación	El nombre de la aplicación activada con el archivo de clave o código de activación.
Restricción de uso de clave	La restricción de uso de la clave (si corresponde).
Brinda acceso a soporte técnico	Información sobre si Kaspersky Lab o uno de nuestros socios proporcionará soporte técnico según los términos de la licencia.
Pestaña "Avanzado"	
Información sobre la licencia	Número de licencia actual.
Información de soporte	Información de contacto de Kaspersky Lab o su socio que proporciona el Servicio de soporte técnico. Este campo puede estar vacío si no se proporciona el Servicio de soporte técnico.
Información del propietario	Información sobre el propietario de la licencia: el nombre del cliente y el nombre de la organización para la cual se adquirió la licencia.

Limitaciones funcionales cuando caduca la licencia

Cuando la licencia actual caduque, se aplicarán las siguientes limitaciones a los componentes funcionales:

- Todas las tareas se detienen, excepto las tareas de Protección de archivos en tiempo real, Análisis a pedido y Control de integridad de la aplicación.
- No puede iniciar ninguna tarea, excepto Protección de archivos en tiempo real, Análisis a pedido y Control de integridad de la aplicación. Estas tareas continúan ejecutándose usando las bases de datos antivirus viejas.
- Se limita la funcionalidad de Prevención de exploits:
  - Los procesos se protegen hasta que se reinician.
  - Los procesos nuevos no se pueden agregar al alcance de la protección.

Otras funciones (repositorios, registros, información de diagnóstico) todavía están disponibles.

Renovación de la licencia

De forma predeterminada, cuando la licencia tiene 14 días restantes antes de su caducidad, Kaspersky Embedded Systems Security lo notifica acerca de la próxima caducidad. En este caso, el estado **Fecha de caducidad de la licencia** se resalta en amarillo en el panel de detalles del nodo **Kaspersky Embedded Systems Security**.

Puede renovar la licencia antes de la fecha de caducidad mediante un archivo de clave adicional o un código de activación. Esto asegura que su equipo permanezca protegido después de la caducidad de la licencia actual y antes de que active la aplicación con una licencia nueva.

► *Para renovar una licencia, siga estos pasos:*

1. Adquiera un nuevo código de activación o un archivo de clave.
2. En el árbol de la Consola de la aplicación, abra el nodo **Licencia**.
3. En el panel de detalles del nodo **Licencia**, realice una de las siguientes acciones:
   - Si desea renovar una licencia con una clave adicional:
     a. Haga clic en el vínculo **Agregar**.
     b. En la ventana que se abre, haga clic en el botón **Examinar** y seleccione un nuevo archivo de clave con la extensión .key.
     c. Seleccione la casilla de verificación **Usar como clave adicional**.
   - Si desea renovar una licencia con un código de activación:
     a. Haga clic en el vínculo **Agregar código de activación**.
     b. Escriba el código de activación comprado en la ventana que se abre.
     c. Seleccione la casilla de verificación **Usar como clave adicional**.

   Se requiere una conexión a Internet para aplicar el código de activación.
4. Haga clic en **Aceptar**.

La clave adicional se agregará y se aplicará automáticamente cuando venza la licencia actual de Kaspersky Embedded Systems Security.

Eliminación de la clave

Se puede eliminar la clave agregada.

Si una clave adicional se ha agregado a Kaspersky Embedded Systems Security y la clave activa se elimina, la clave adicional se convierte automáticamente en la clave activa.

Si se elimina una clave adicional, se puede restaurar volviendo a aplicar el archivo de clave.

► *Para eliminar una clave que se ha agregado:*

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Licencia**.
2. En el panel de detalles del nodo **Licencia**, en la tabla que contiene información sobre claves agregadas,

seleccione la clave que desea eliminar.

3. En el menú contextual de la línea que contiene información sobre la clave seleccionada, seleccione **Eliminar**.
4. Haga clic en el botón **Sí** de la ventana de confirmación para confirmar que desea eliminar la clave.

Se eliminará la clave seleccionada.

Cómo usar el Complemento de administración

Esta sección proporciona información sobre el Complemento de administración de Kaspersky Embedded Systems Security y describe cómo administrar la aplicación instalada en un equipo protegido o en un grupo de equipos.

En este capítulo

Administración de Kaspersky Embedded Systems Security mediante Kaspersky Security Center

Puede administrar de forma centralizada varios equipos si Kaspersky Embedded Systems Security está instalado e incluido en un grupo de administración por medio del Complemento de administración de Kaspersky Embedded Systems Security. Kaspersky Security Center también le permite ajustar, por separado, los parámetros de configuración de operación de cada equipo incluido en el grupo de administración.

El grupo de administración se crea de forma manual en Kaspersky Security Center e incluye varios equipos con Kaspersky Embedded Systems Security instalado, para los cuales es conveniente configurar las mismas opciones de control y protección. Para obtener más información sobre la utilización de grupos de administración, consulte la *Ayuda de Kaspersky Security Center*.

La configuración de la aplicación para un equipo no está disponible si el funcionamiento de Kaspersky Embedded Systems Security en ese equipo es controlado por una directiva de Kaspersky Security Center activa.

Kaspersky Embedded Systems Security puede administrarse desde Kaspersky Security Center de las siguientes maneras:

- **Utilización de directivas de Kaspersky Security Center**. Es posible usar directivas de Kaspersky Security Center para configurar remotamente la misma configuración de protección para un grupo de equipos. La configuración de la tarea especificada en la directiva activa tiene prioridad sobre las opciones de la tarea configuradas localmente en la Consola de la aplicación o remotamente en la ventana **Propiedades: <Nombre del equipo>** de Kaspersky Security Center.

  Puede usar directivas para establecer la configuración general de la aplicación, la configuración de la tarea Protección en tiempo real, la configuración de las tareas de Control de actividad local, la configuración del inicio de las tareas del sistema programadas y la configuración de uso del perfil.

- **Utilización de tareas de grupo de Kaspersky Security Center**. Las tareas de grupo de Kaspersky Security Center permiten configurar a distancia las opciones comunes de las tareas que tienen un periodo de vencimiento para un grupo de equipos.
- Puede usar tareas de grupo para activar la aplicación, configurar la tarea de Análisis a pedido, actualizar la configuración de tareas y configurar la tarea Generador de reglas para Control de inicio de aplicaciones.
- **Utilización de tareas para un conjunto de dispositivos**. Las tareas para un conjunto de dispositivos permiten la configuración remota de las opciones comunes de las tareas con un periodo de ejecución limitado para equipos que no pertenecen a ninguno de los grupos de administración.
- **Utilización de la ventana Propiedades de un solo equipo**. En la ventana **Propiedades: <Nombre del equipo>** puede configurar remotamente las opciones de tareas para un solo equipo incluido en el grupo de administración. Puede establecer tanto la configuración general de la aplicación como la configuración de todas las tareas de Kaspersky Embedded Systems Security si el equipo seleccionado no es controlado por una directiva de Kaspersky Security Center activa.

Kaspersky Security Center hace posible configurar los parámetros de la aplicación y las funciones avanzadas, y le permite trabajar con registros y notificaciones. Puede configurar estos parámetros tanto para un grupo de equipos, como para un equipo en particular.

Administración de las configuraciones de la aplicación

Esta sección contiene información acerca de cómo ajustar las configuraciones generales de Kaspersky Embedded Systems Security en Kaspersky Security Center.

En este capítulo

Administración de Kaspersky Embedded Systems Security mediante Kaspersky Security Center

Puede administrar de forma centralizada varios equipos si Kaspersky Embedded Systems Security está instalado e incluido en un grupo de administración por medio del Complemento de administración de Kaspersky Embedded Systems Security. Kaspersky Security Center también le permite ajustar, por separado, los parámetros de configuración de operación de cada equipo incluido en el grupo de administración.

El grupo de administración se crea de forma manual en Kaspersky Security Center e incluye varios equipos con Kaspersky Embedded Systems Security instalado, para los cuales es conveniente configurar las mismas opciones de control y protección. Para obtener más información sobre la utilización de grupos de administración, consulte la *Ayuda de Kaspersky Security Center*.

La configuración de la aplicación para un equipo no está disponible si el funcionamiento de Kaspersky Embedded Systems Security en ese equipo es controlado por una directiva de Kaspersky Security Center activa.

Kaspersky Embedded Systems Security puede administrarse desde Kaspersky Security Center de las siguientes maneras:

- **Utilización de directivas de Kaspersky Security Center**. Es posible usar directivas de Kaspersky Security Center para configurar remotamente la misma configuración de protección para un grupo de equipos. La configuración de la tarea especificada en la directiva activa tiene prioridad sobre las opciones de la tarea configuradas localmente en la Consola de la aplicación o remotamente en la ventana **Propiedades: <Nombre del equipo>** de Kaspersky Security Center.

  Puede usar directivas para establecer la configuración general de la aplicación, la configuración de la tarea Protección en tiempo real, la configuración de las tareas de Control de actividad local, la configuración del inicio de las tareas del sistema programadas y la configuración de uso del perfil.

- **Utilización de tareas de grupo de Kaspersky Security Center**. Las tareas de grupo de Kaspersky Security Center permiten configurar a distancia las opciones comunes de las tareas que tienen un periodo de vencimiento para un grupo de equipos.

- Puede usar tareas de grupo para activar la aplicación, configurar la tarea de Análisis a pedido, actualizar la configuración de tareas y configurar la tarea Generador de reglas para Control de inicio de aplicaciones.

- **Utilización de tareas para un conjunto de dispositivos**. Las tareas para un conjunto de dispositivos permiten la configuración remota de las opciones comunes de las tareas con un periodo de ejecución limitado para equipos que no pertenecen a ninguno de los grupos de administración.

- **Utilización de la ventana Propiedades de un solo equipo**. En la ventana **Propiedades: <Nombre del equipo>** puede configurar remotamente las opciones de tareas para un solo equipo incluido en el grupo de administración. Puede establecer tanto la configuración general de la aplicación como la configuración de todas las tareas de Kaspersky Embedded Systems Security si el equipo seleccionado no es controlado por una directiva de Kaspersky Security Center activa.

Kaspersky Security Center hace posible configurar los parámetros de la aplicación y las funciones avanzadas, y le permite trabajar con registros y notificaciones. Puede configurar estos parámetros tanto para un grupo de equipos, como para un equipo en particular.

Navegación

Sepa cómo navegar a la configuración de la tarea requerida a través de la interfaz.

En esta sección

Cómo abrir la configuración general mediante la directiva

► *Para abrir la configuración de la aplicación de Kaspersky Embedded Systems Security mediante la*

directiva:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas.**
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades:** se abre la ventana **<Nombre de la directiva>**, allí seleccione la sección **Configuración de la aplicación**.
6. Haga clic en el botón **Configuración** en la subsección de la configuración que desea ajustar.

Cómo abrir la configuración general en la ventana de propiedades de la aplicación

► *Para abrir la ventana de propiedades de Kaspersky Embedded Systems Security para un solo equipo:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Dispositivos**.
4. Abra la ventana **Propiedades: <Nombre del equipo>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre del equipo protegido
   - Seleccione el elemento **Propiedades** en el menú contextual del equipo protegido.

   Se abre la ventana **Propiedades:** Se abre la ventana **<Nombre del equipo>**.
5. En la sección **Aplicaciones**, seleccione **Kaspersky Embedded Systems Security**.
6. Haga clic en el botón **Propiedades**.

   Se abrirá la ventana **Configuración de aplicación de "Kaspersky Embedded Systems Security"**.
7. Seleccione la sección **Configuración de la aplicación**.

Configuración de las opciones generales de la aplicación en Kaspersky Security Center

Puede establecer la configuración general de Kaspersky Embedded Systems Security desde Kaspersky Security Center para un grupo de equipos o para un equipo.

En esta sección

Configuración de escalabilidad y de la interfaz en Kaspersky Security Center

► *Para ajustar la configuración de la escalabilidad y la interfaz de aplicación:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas" en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center" en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.
4. En la sección **Configuración de la aplicación**, en el bloque **Escalabilidad e interfaz**, haga clic en **Configuración**.
5. En la ventana **Configuración avanzada de la aplicación** en la pestaña **General**, establezca la siguiente configuración:
   - En la sección **Configuración de escalabilidad**, establezca la configuración que define el número de procesos usados por Kaspersky Embedded Systems Security:
     - **Detectar automáticamente la configuración de escalabilidad**.

       Kaspersky Embedded Systems Security regula automáticamente el número de procesos usados.

       Este es el valor predeterminado.
     - **Configurar manualmente el número de procesos de trabajo**.

       Kaspersky Embedded Systems Security regula la cantidad de procesos en funcionamiento activos según los valores especificados.
       - **Número máximo de procesos activos.**

         Número máximo de procesos que utiliza Kaspersky Embedded Systems Security. El campo de entrada se encuentra disponible si se selecciona la opción **Configurar manualmente el número de procesos de trabajo**.
       - **Número de procesos para la protección en tiempo real.**

         Número máximo de procesos usados por los componentes de la tarea Protección en tiempo real. El campo de entrada se encuentra disponible si se selecciona la opción **Configurar manualmente el número de procesos de trabajo**.
       - **Número de procesos para tareas de Análisis a pedido en segundo plano.**

         Número máximo de procesos usados por el componente de Análisis a pedido al ejecutar tareas de Análisis a pedido en segundo plano. El campo de entrada se encuentra disponible si se selecciona la opción **Configurar manualmente el número de procesos**

de trabajo.

- En la sección **Interacción con el usuario**, configure la visualización del icono de la bandeja del sistema en el área de notificación: seleccione o desactive la casilla de verificación **Mostrar icono de la bandeja del sistema en la barra de tareas**.

6. En la pestaña **Depósito jerárquico**, seleccione la opción para acceder al depósito jerárquico.
7. Haga clic en **Aceptar**.

Se guarda la configuración de la aplicación.

Configuración de opciones de seguridad en Kaspersky Security Center

► *Para configurar los valores de seguridad manualmente, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.
4. En la sección **Configuración de la aplicación**, haga clic en el botón **Configurar** en la configuración de **Seguridad**.
5. En la ventana **Configuración de seguridad**, configure las siguientes opciones:
   - En la sección **Configuración de confiabilidad**, establezca la configuración de la recuperación de las tareas de Kaspersky Embedded Systems Security cuando la aplicación devuelva un error o deje de funcionar.
     - **Ejecutar recuperación de tarea**

       Esta casilla de verificación habilita o deshabilita la recuperación de las tareas de Kaspersky Embedded Systems Security cuando la aplicación devuelve un error o deja de funcionar.

       Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security recupera automáticamente las tareas de Kaspersky Embedded Systems Security cuando la aplicación devuelve un error o deja de funcionar.

       Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no recupera las tareas de Kaspersky Embedded Systems Security cuando la aplicación devuelve un error o deja de funcionar.

       De forma predeterminada, la casilla está activada.

- **Recuperar tareas de análisis a pedido no más de (veces)**

  Número de intentos para recuperar una tarea de Análisis a pedido después de que Kaspersky Embedded Systems Security devuelve un error. El campo de entrada se encuentra disponible si se activa la casilla **Ejecutar recuperación de tarea**.

- En la sección **Acciones si se pasa a un sistema de alimentación de respaldo (UPS)**, especifique limitaciones de la carga del equipo creadas por Kaspersky Embedded Systems Security después de cambiar a la alimentación de UPS:

  - **No iniciar las tareas de análisis programadas**

    Esta casilla de verificación habilita o deshabilita el inicio de una tarea de análisis programada después de que el equipo cambia a una fuente de UPS hasta que el modo de suministro de energía estándar se restaura.

    Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security no inicia tareas de análisis programadas después de que el equipo cambia a una fuente de UPS hasta que el modo de suministro de energía estándar se restaura.

    Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security inicia tareas de análisis programadas sin tener en cuenta el modo de suministro de energía.

    De forma predeterminada, la casilla está activada.

  - **Detener las tareas de análisis en curso**

    La casilla de verificación habilita o deshabilita la ejecución de tareas de análisis en ejecución después de que el equipo cambia a una fuente de UPS.

    Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security pausa las tareas de análisis en ejecución después de que el equipo cambia a una fuente de UPS.

    Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security continúa las tareas de análisis en ejecución después de que el equipo cambia a una fuente de UPS.

    De forma predeterminada, la casilla está activada.

- En la sección **Ajustes de protección mediante contraseña**, establezca una contraseña para proteger el acceso a las funciones de Kaspersky Embedded Systems Security.

6. Haga clic en **Aceptar**.

Se guarda la configuración establecida de escalabilidad y de confiabilidad.

Configuración de opciones de conexión mediante Kaspersky Security Center

Los parámetros de conexión configurados se utilizan para conectar Kaspersky Embedded Systems Security a servidores de activación y actualización durante la integración de aplicaciones con Servicios KSN.

► *Para configurar los parámetros de conexión, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas" en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center" en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.

4. En la sección **Configuración de la aplicación**, haga clic en el botón **Configurar** en el bloque **Conexiones**.

   Se abrirá la ventana **Configuración de conexión**.

5. En la ventana **Configuración de conexión**, configure las siguientes opciones:
   - En la sección **Configuración del servidor proxy**, seleccione la configuración de uso del servidor proxy:
     - **No usar un servidor proxy**.

       Si esta opción está seleccionada, Kaspersky Embedded Systems Security se conecta a Servicios KSN directamente, sin usar ningún servidor proxy.
     - **Usar la configuración especificada del servidor proxy**.

       Si esta opción está seleccionada, Kaspersky Embedded Systems Security se conecta al KSN con la configuración del servidor proxy especificada manualmente.
     - La dirección IP o el nombre del símbolo del servidor proxy y el número de puerto.
     - **No usar el servidor proxy para las direcciones locales**.

       La casilla de verificación habilita o deshabilita el uso de un servidor proxy al acceder a equipos ubicados en la misma red que el equipo con Kaspersky Embedded Systems Security instalado.

       Si esta casilla de verificación está seleccionada, se accede a los equipos directamente desde la red, que aloja el equipo con Kaspersky Embedded Systems Security instalado. No se utiliza ningún servidor proxy.

       Si la casilla de verificación está desactivada, se aplica el servidor proxy para la conexión a equipos locales.

       De forma predeterminada, la casilla está activada.
   - En la sección **Configuración de autenticación del servidor proxy**, especifique la configuración de autenticación:
     - Seleccione la configuración de autenticación en la lista desplegable.

- **No usar autenticación**: no se realiza la autenticación. Este modo está seleccionado en forma predeterminada.
- **Usar autenticación NTLM**: la autenticación se realiza usando el protocolo de autenticación de red NTLM desarrollado por Microsoft.
- **Usar autenticación NTLM con nombre de usuario y contraseña**: la autenticación se realiza usando el nombre y la contraseña a través del protocolo de autenticación de red NTLM desarrollado por Microsoft.
- **Aplicar nombre de usuario y contraseña**: la autenticación se realiza usando el nombre de usuario y contraseña.

- Escriba el nombre de usuario y la contraseña, de ser necesario.

- En el bloque **Licencia**, desactive o seleccione **Usar Kaspersky Security Center como servidor proxy al activar la aplicación**.

6. Haga clic en **Aceptar**.

Los parámetros de conexión configurados se guardan.

Configuración del inicio programado de las tareas locales del sistema

Puede usar directivas para autorizar o bloquear el inicio de las tareas de Análisis a pedido y de Actualización del sistema local según la siguiente programación configurada localmente en cada equipo en el grupo de administración:

- Si el inicio programado de un tipo específico de tarea local del sistema está prohibido por una directiva, estas tareas no se realizarán en el equipo local según la programación. Puede iniciar las tareas locales del sistema manualmente.
- Si el inicio programado de un tipo específico de tarea local del sistema está permitido por una directiva, estas tareas se realizarán según los parámetros programados y configurados localmente para esta tarea.

De forma predeterminada, el inicio de tareas locales del sistema está prohibido por la directiva.

Recomendamos que no habilite el inicio de tareas locales del sistema si las actualizaciones o los análisis a pedido están siendo administrados por tareas de grupo de Kaspersky Security Center.

Si no usa las tareas actualización de grupo o análisis a pedido, permita que tareas locales del sistema se inicien en la directiva: Kaspersky Embedded Systems Security realizará la base de datos de la aplicación y actualizaciones del módulo, e iniciará todas las tareas de análisis a pedido del sistema local de acuerdo con la programación predeterminada.

Puede usar directivas para autorizar o bloquear el inicio programado de las siguientes tareas del sistema locales:

- Tareas de Análisis a pedido: Análisis de áreas críticas, Análisis de archivos en cuarentena, Análisis al inicio del sistema operativo, Control de integridad de la aplicación.
- Tareas de actualización: Actualización de bases de datos, Actualización de módulos del programa y Copia de actualizaciones.

Si el equipo protegido se excluye del grupo de administración, la programación de tareas del sistema se habilitará automáticamente.

► *Para autorizar o bloquear el inicio programado de tareas del sistema de Kaspersky Embedded Systems Security en una directiva, siga estos pasos:*

1. En el nodo **Dispositivos administrados** del árbol de la consola de administración, expanda el grupo requerido y seleccione la pestaña **Directivas**.
2. En la pestaña **Directivas**, en el menú contextual de la directiva para la que desea configurar el inicio programado de tareas del sistema de Kaspersky Embedded Systems Security en el grupo de equipos, seleccione el elemento **Propiedades**
3. En la ventana **Propiedades: <Nombre de la directiva>**, abra la sección **Configuración de la aplicación**. En la sección **Ejecutar tareas del sistema**, haga clic en el botón **Configurar** y realice lo siguiente:
   - Seleccione las casillas de verificación **Permitir que se inicien las tareas de análisis a pedido** y **Permitir que se inicien las tareas de actualización y de Copia de actualizaciones** para autorizar el inicio programado de estas tareas.
   - Desactive las casillas de verificación **Permitir que se inicien las tareas de análisis a pedido** y **Permitir que se inicien las tareas de actualización y de Copia de actualizaciones** para deshabilitar el inicio programado estas tareas.

   La selección o la desactivación de la casilla de verificación no afectará la configuración del inicio de ninguna tarea local personalizada de este tipo.
4. Asegúrese de que la directiva que configura esté activa y se aplique al grupo de equipos seleccionado.
5. Haga clic en **Aceptar**.

La configuración del inicio de la tarea programada establecida se aplica para las tareas seleccionadas.

Configuración de opciones de Cuarentena y Copia de seguridad en Kaspersky Security Center

► *Para establecer la configuración general de Copia de seguridad en Kaspersky Security Center:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.

3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas" en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center" en la página 117).

   > Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.

4. En la sección **Adicional**, haga clic en el botón **Configurar** de la subsección **Depósitos**.
5. Use la pestaña **Copia de seguridad** de la ventana de configuración de **Depósitos** para configurar las siguientes opciones de Copia de seguridad:

   - Para especificar la **Carpeta de Copia de seguridad**, utilice el campo de la carpeta Copia de seguridad para seleccionar la carpeta requerida en la unidad local del equipo protegido o introduzca la ruta completa.
   - Para establecer el tamaño máximo de Copia de seguridad, seleccione la casilla de verificación **Tamaño máx. de copia de seguridad (MB)** y especifique el valor necesario en megabytes en el campo de entrada.
   - Para establecer el valor umbral de espacio libre en Copia de seguridad, defina el valor de la opción **Tamaño máx. de copia de seguridad (MB)**, seleccione la casilla de verificación **Valor umbral de espacio disponible (MB)** y especifique el valor mínimo de espacio libre en la carpeta de Copia de seguridad en megabytes.
   - Para especificar una carpeta para objetos restaurados, seleccione la carpeta correspondiente en la unidad local del equipo protegido en la sección **Configuración de restauración** o introduzca el nombre de la carpeta y su ruta completa en el campo **Carpeta de destino para restaurar objetos**.

6. En la ventana de configuración de **Depósitos** de la pestaña **Cuarentena**, configure las siguientes opciones de **Cuarentena**:

   - Para cambiar la carpeta de cuarentena, en el campo de entrada de la **carpeta de Cuarentena** especifique la ruta completa de la carpeta en el disco local del equipo protegido.
   - Para establecer el tamaño máximo de Cuarentena, seleccione la casilla de verificación **Tamaño máximo de cuarentena (MB)** y especifique el valor de este parámetro en megabytes en el campo de entrada.
   - Para establecer la cantidad mínima de espacio libre en la Cuarentena, seleccione la casilla de verificación **Tamaño máximo de cuarentena (MB)**, la casilla de verificación **Valor umbral de espacio disponible (MB)** y, a continuación, especifique el valor de este parámetro en megabytes en el campo de entrada.
   - Para cambiar la carpeta de almacenamiento de los objetos restaurados de la cuarentena, en el campo de entrada **Carpeta de destino para restaurar objetos**, especifique la ruta completa de la carpeta en el disco local del equipo protegido.

7. Haga clic en **Aceptar**.

Los parámetros configurados de la Cuarentena y las Copia de seguridad se guardan.

Configuración de registros y notificaciones

La consola de administración de Kaspersky Security Center se puede usar para configurar las notificaciones para el administrador y los usuarios sobre los eventos futuros relacionados con Kaspersky Embedded Systems Security y el estado de la protección antivirus en el equipo protegido:

- El administrador puede recibir información sobre eventos de tipos seleccionados;
- Los usuarios de la LAN que tienen acceso al equipo protegido y los usuarios del equipo de terminales pueden recibir información sobre eventos del tipo *Objeto detectado*.

Es posible configurar notificaciones sobre eventos de Kaspersky Embedded Systems Security para un solo equipo en la ventana **Propiedades: <Nombre del equipo>** del equipo seleccionado, o para un grupo de equipos en la ventana **Propiedades: <Nombre de directiva>** del grupo de administración seleccionado.

En la pestaña **Notificaciones de eventos** o en la ventana **Configuración de notificaciones**, puede configurar los siguientes tipos de notificaciones:

- Las notificaciones para el administrador sobre eventos de tipos seleccionados se pueden configurar mediante la pestaña **Notificaciones de eventos** (la pestaña estándar de la aplicación Kaspersky Security Center). Para obtener más información sobre los métodos de notificación, consulte la *Ayuda de Kaspersky Security Center*.
- Las notificaciones para el administrador y para los usuarios se pueden configurar en la ventana **Configuración de notificaciones**.

Puede configurar notificaciones para algunos tipos de eventos en la ventana o en la pestaña solamente; y puede usar tanto la ventana como la pestaña para configurar notificaciones para otros tipos de eventos.

Si configura las notificaciones sobre eventos del mismo tipo usando el mismo modo en la pestaña **Notificaciones de eventos** y en la ventana **Configuración de notificaciones**, el administrador del sistema recibirá las notificaciones de esos eventos dos veces, pero en el mismo modo.

En esta sección

Configuración del registro

► *Para configurar los registros de Kaspersky Embedded Systems Security, realice los siguientes pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas" en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center" en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.
4. En la sección **Registros y notificaciones**, haga clic en el botón **Configurar** en el bloque **Registros de tareas**.
5. En la ventana **Configuración de registros**, defina la siguiente configuración de Kaspersky Embedded Systems Security según sus requisitos:
   - Configure el nivel de detalle de los eventos en los registros. Para ello, realice las siguientes acciones:
     a. En la lista **Componente**, seleccione el componente de Kaspersky Embedded Systems Security para el cual desea configurar el nivel de detalle.
     b. Para definir el nivel de detalle en los registros de tareas y el registro de auditoría del sistema para el componente seleccionado, elija el nivel necesario en **Nivel de importancia**.
   - Para cambiar la ubicación predeterminada de los registros, especifique la ruta completa a la carpeta o haga clic en el botón **Examinar** para seleccionarla.
   - Especifique la cantidad de días que se almacenarán los registros de tareas.
   - Especifique durante cuantos días se almacenará la información que se muestra en el nodo **Registro de auditoría del sistema**.
6. Haga clic en **Aceptar**.

Los parámetros de registro configurados se guardaron.

Registro de seguridad

Kaspersky Embedded Systems Security mantiene un registro de eventos asociados con la violación de la seguridad o los intentos de violación de la seguridad en el equipo protegido. Los siguientes eventos se incluyen en este registro:

- Eventos de Prevención de exploits.
- Eventos de inspección de registros críticos
- Los eventos críticos que indican un intento de violación de la seguridad (para la Protección del equipo en tiempo real, el Análisis a pedido, el Monitor de integridad de archivos, el Control de inicio de aplicaciones y las tareas de Control de dispositivos).

Puede cancelar la selección del registro de seguridad, al igual que el Registro de auditoría del sistema (consulte la sección “Eliminación de eventos del registro de auditoría del sistema” en la página 200). Además, Kaspersky Embedded Systems Security registra eventos de auditoría del sistema relacionados con el borrado del registro de seguridad.

Configuración de las opciones de integración de SIEM

Para reducir la carga en dispositivos de rendimiento reducido y reducir el riesgo de la degradación del sistema a consecuencia de volúmenes aumentados de registros de la aplicación, puede configurar la publicación de eventos de auditoría y eventos de rendimiento de la tarea en el *servidor syslog* mediante el protocolo Syslog.

Un servidor syslog es un servidor externo para agregar eventos (SIEM). Obtiene y analiza eventos recibidos y también realiza otras acciones para administrar registros.

Puede usar la integración de SIEM en dos modos:

- Duplicar eventos en el servidor syslog: este modo indica que todos los eventos de rendimiento de la tarea cuya publicación se configura en la configuración de registros, así como todos los eventos de auditoría del sistema, continúen almacenándose en el equipo local hasta después de que se envíen a SIEM.

  Se recomienda usar este modo para reducir máximamente la carga en el equipo protegido.

- Eliminar copias locales de eventos: este modo indica que todos los eventos que se registran durante el funcionamiento de la aplicación y se publican en SIEM se eliminen del equipo local.

  La aplicación nunca elimina las versiones locales del registro de seguridad.

Kaspersky Embedded Systems Security puede convertir eventos en los registros de la aplicación a formatos admitidos por el servidor syslog, de modo que dichos eventos se puedan transmitir y sean reconocidos de manera exitosa por SIEM. La aplicación admite la conversión al formato de datos estructurado y al formato JSON.

Para reducir el riesgo de transmisión no exitosa de eventos a SIEM, puede definir la configuración para conectar al espejo syslog idéntico.

El servidor syslog idéntico es un servidor syslog adicional al cual la aplicación cambia automáticamente si la conexión con el servidor syslog principal no está disponible o si el servidor principal no se puede utilizar.

De forma predeterminada, la integración de SIEM no se usa. Puede habilitar y deshabilitar la integración de SIEM y configurar las opciones de funcionalidad (consulte la tabla a continuación).

Tabla 10. Configuración de integración de SIEM

Configuración	Valor predeterminado	Descripción
Enviar eventos a un servidor remoto de Syslog, mediante el protocolo de Syslog	No aplicado	Puede habilitar o deshabilitar la integración de SIEM al seleccionar o al desactivar la casilla, respectivamente.
Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog	No aplicado	Puede ajustar la configuración para almacenar copias locales de registros después de que se envíen a SIEM al seleccionar o al desactivar la casilla.
Formato de los eventos	Datos estructurados	Puede seleccionar uno de dos formatos a los cuales la aplicación convierte sus eventos antes de enviarlos al servidor syslog para el mejor reconocimiento de estos eventos por SIEM.
Protocolo de conexión	TCP	Puede usar la lista desplegable para configurar la conexión con el servidor syslog principal mediante protocolos TCP o UDP; o con el servidor syslog idéntico mediante el protocolo TCP.
Configuración de conexión al servidor syslog principal	Dirección IP: 127.0.0.1 Puerto: 514	Puede usar los campos apropiados para configurar la dirección IP y el puerto usados para conectarse al servidor syslog principal. Puede especificar la dirección IP solo en el formato IPv4.
Utilice el servidor reflejado de Syslog si no es posible acceder al servidor principal	No aplicado	Puede usar la casilla para habilitar o deshabilitar el uso de un servidor syslog idéntico.
Configuración de conexión al servidor syslog idéntico	Dirección IP: 127.0.0.1 Puerto: 514	Puede usar los campos apropiados para configurar la dirección IP y el puerto usados para conectarse al servidor reflejado de Syslog. Puede especificar la dirección IP solo en el formato IPv4.

► *Para configurar la integración de SIEM:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

> Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.

4. En la sección **Registros y notificaciones**, haga clic en el botón **Configurar** en el bloque **Registros de tareas**.

   Se abre la ventana **Configuración de registros y notificaciones**.

5. Seleccione la pestaña **Integración de SIEM**.

6. En la sección **Ajustes de integración**, seleccione la casilla **Enviar eventos a un servidor remoto de Syslog, mediante el protocolo de Syslog**.

   La casilla habilita o deshabilita la funcionalidad para enviar eventos publicados a un servidor syslog externo.

   Si la casilla se selecciona, la aplicación envía eventos publicados a SIEM según la configuración de integración de SIEM establecida.

   Si la casilla se desactiva, la aplicación no realiza la integración de SIEM. No puede ajustar la configuración de integración de SIEM si la casilla se desactiva.

   De forma predeterminada, la casilla está desactivada.

7. Si es necesario, en la sección **Ajustes de integración**, seleccione la casilla **Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog**.

   La casilla habilita o deshabilita la eliminación de copias locales de registros cuando se envían a SIEM.

   Si la casilla se selecciona, la aplicación elimina las copias locales de eventos después de que se han publicado correctamente en SIEM. Este modo se recomienda en equipos de rendimiento reducido.

   Si la casilla se desactiva, la aplicación solo envía eventos a SIEM. Las copias de los de registros continúan almacenándose a nivel local.

   De forma predeterminada, la casilla está desactivada.

> El estado de la casilla **Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog** no afecta la configuración para almacenar eventos del registro de seguridad: la aplicación nunca elimina automáticamente eventos del registro de seguridad.

8. En la sección **Formato de los eventos**, especifique el formato al cual desea convertir los eventos operativos de la aplicación de modo que se puedan enviar a SIEM.

   De forma predeterminada, la aplicación los convierte en el formato de datos estructurado.

9. En la sección **Configuración de conexión**:

   - Especifique el protocolo de conexión de SIEM.
   - Especifique la configuración para conectarse al servidor syslog principal.

     Puede especificar una dirección IP en formato IPv4 únicamente.

- Seleccione la casilla **Utilice el servidor reflejado de Syslog si no es posible acceder al servidor principal** si desea que la aplicación use otra configuración de conexión cuando sea incapaz de enviar eventos al servidor syslog principal.
  - Especifique la siguiente configuración para conectarse al servidor syslog idéntico: **Dirección IP** y **Puerto**.

    Los campos **Dirección IP** y **Puerto** para el servidor syslog idéntico no se pueden modificar si se desactiva la casilla **Utilice el servidor reflejado de Syslog si no es posible acceder al servidor principal**.

    Puede especificar una dirección IP en formato IPv4 únicamente.

10. Haga clic en **Aceptar**.

La configuración de integración de SIEM establecida se aplicará.

Configuración de las opciones de notificación

► *Para configurar las notificaciones de Kaspersky Embedded Systems Security, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.
4. En la sección **Registros y notificaciones**, haga clic en el botón **Configurar** en la subsección **Notificaciones de eventos**.
5. En la ventana **Configuración de notificaciones**, defina la siguiente configuración de Kaspersky Embedded Systems Security según sus requisitos:
   - En la lista **Configuración de notificaciones**, seleccione el tipo de notificación cuya configuración desea establecer.
   - En la sección **Notificar a los usuarios**, configure el método de notificación a los usuarios. Si es necesario, escriba el texto del mensaje de notificación.
   - En la sección **Notificar a los administradores**, configure el método de notificación al administrador. Si es necesario, escriba el texto del mensaje de notificación. Si es necesario, establezca la configuración de notificaciones adicionales con un clic en el botón **Configurar**.
   - En la sección **Umbrales de generación de eventos**, especifique los intervalos de tiempo después de

los cuales Kaspersky Embedded Systems Security registra los eventos *La base de datos de la aplicación está desactualizada, La base de datos de la aplicación está obsoleta* y *Hace mucho tiempo que no se realiza un análisis de áreas críticas*.

- **La base de datos de la aplicación está desactualizada (días)**

  Número de días que han pasado desde la última actualización de bases de datos.

  El valor predeterminado es 7 días.

- **La base de datos de la aplicación es obsoleta (días)**

  Número de días que han pasado desde la última actualización de bases de datos.

  El valor predeterminado es 14 días.

- **Hace mucho tiempo que no se realiza un análisis de áreas críticas (días)**

  La cantidad de días después del último Análisis de áreas críticas satisfactorio.

  El valor predeterminado es 30 días.

6. Haga clic en **Aceptar**.

La configuración de notificaciones se guarda.

Configuración de la interacción con el servidor de administración

► *Para seleccionar los tipos de objetos sobre los cuales Kaspersky Embedded Systems Security envía información al Servidor de administración de Kaspersky Security Center:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.

4. En la sección **Registros y notificaciones**, haga clic en el botón **Configurar** en el bloque **Interacción con Servidor de administración**.

   La ventana **Lista de la red de servidores de administración** se abre.

5. En la ventana **Lista de la red de servidores de administración** seleccione los tipos de objetos sobre los cuales Kaspersky Embedded Systems Security enviará la información al Servidor de administración de Kaspersky Security Center:

   - Objetos en Cuarentena.
   - Objetos con Copia de seguridad.

6. Haga clic en **Aceptar**.

   Kaspersky Embedded Systems Security enviará información sobre los tipos de objeto seleccionados al Servidor de administración.

Creación y configuración de directivas

Esta sección proporciona información sobre la utilización de directivas de Kaspersky Security Center para administrar Kaspersky Embedded Systems Security en varios equipos.

Las directivas globales de Kaspersky Security Center pueden crearse para administrar la protección de varios equipos en los que está instalado Kaspersky Embedded Systems Security.

Una directiva implementa la configuración, las funciones y tareas de Kaspersky Embedded Systems Security especificadas en la misma en todos los equipos protegidos para un grupo de administración.

Se pueden crear e implementar por turnos varias directivas para un grupo de administración. En la Consola de administración, la directiva activa actualmente para un grupo tiene el estado *activa*.

La información sobre la implementación de la directiva se carga en el registro de auditoría del sistema de Kaspersky Embedded Systems Security. Esta información se puede visualizar en la Consola de la aplicación, en el nodo **Registro de auditoría del sistema**.

Kaspersky Security Center ofrece una manera de aplicar directivas en equipos locales: *Prohibir cambiar la configuración*. Después de aplicar una directiva, Kaspersky Embedded Systems Security utiliza los valores de configuración al lado de los cuales ha seleccionado el icono en las propiedades de la directiva en equipos locales, en lugar de los valores de configuración previos a la aplicación de la directiva. Kaspersky Embedded Systems Security no aplica los valores de configuración de la directiva activa al lado de los cuales ha seleccionado el icono en las propiedades de la directiva.

Si una directiva está activa, los valores de configuración marcados con el icono en la directiva se muestran en la Consola de la aplicación, pero no se pueden modificar. Los valores de otras opciones de configuración (marcados con el icono en la directiva) pueden modificarse en la Consola de la aplicación.

La configuración establecida en la directiva activa y marcada con el icono también bloquea los cambios en Kaspersky Security Center para un equipo en la ventana **Propiedades: <Nombre del equipo>**.

La configuración que se especifica y se envía al equipo local usando una directiva activa se guarda en la configuración de las tareas locales después de que se deshabilita la directiva activa.

Si la directiva define la configuración para una tarea de Protección del equipo en tiempo real y si dicha tarea se está ejecutando en ese momento, la configuración definida por la directiva se modificará en cuanto se aplique la

directiva. Si la tarea no está en ejecución, la configuración se implementará cuando se inicie.

En este capítulo

Creación de una directiva

El proceso de creación de una directiva implica los siguientes pasos:

1. Crear una directiva mediante el asistente para creación de directivas. Las tareas de configuración de la Protección del equipo en tiempo real pueden establecerse mediante los cuadros de diálogo del asistente.
2. Establecer la configuración de la directiva. En la ventana **Propiedades: <Nombre de la directiva>** de la directiva creada, puede definir la configuración de las tareas de Protección del equipo en tiempo real, la configuración general de Kaspersky Embedded Systems Security, la configuración de la Cuarentena y la Copia de seguridad, el nivel de detalle para los registros de tareas y las notificaciones de administrador y de usuario sobre eventos de Kaspersky Embedded Systems Security.

► *Para crear una directiva para un grupo de equipos que ejecutan la aplicación instalada de Kaspersky Embedded Systems Security, realice los siguientes pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la consola de administración de Kaspersky Security Center y, a continuación, seleccione el grupo de administración que contiene los equipos para los que desea crear una directiva.
2. En el panel de detalles del grupo de administración seleccionado, seleccione la pestaña **Directivas** y haga clic en el vínculo **Crear una directiva** para iniciar el asistente y crear una directiva.

   Se abre la ventana **Nuevo asistente de directiva**.
3. En la ventana **Seleccionar la aplicación para la cual desea crear una directiva de grupo**, seleccione Kaspersky Embedded Systems Security y haga clic en **Siguiente**.
4. Ingrese un Nombre de la directiva de grupo en el campo **Nombre**.

   El nombre de la directiva no puede contener los siguientes símbolos: **"** * < : > ? \ | .
5. Para aplicar la configuración de la directiva usada para la versión anterior de la aplicación:
   a. Seleccione la casilla de verificación **Usar configuración de la directiva para versiones anteriores de la aplicación**.
   b. Haga clic en el botón **Seleccionar**.
   c. Seleccione la directiva que desea aplicar.
   d. Haga clic en **Siguiente**.
6. En la ventana **Selección del tipo de operación**, seleccione una de las siguientes opciones:
   - **Nueva**, para crear una directiva nueva con las opciones predeterminadas.

- **Importar directiva creada con versiones anteriores de Kaspersky Embedded Systems Security**, para usar la directiva de esa versión como plantilla.
- Haga clic en **Examinar** y seleccione un archivo de configuración donde esté almacenada una directiva existente.

7. En la ventana **Protección del equipo en tiempo real**, configure la Protección de archivos en tiempo real, las tareas de Uso de KSN y la funcionalidad de Prevención de exploits como se requiere. Autorice o bloquee el uso de tareas de directivas configuradas en equipos locales en la red:
   - Haga clic en el botón para autorizar cambios en la configuración de tareas en equipos en red y bloquear la aplicación de la configuración de tareas establecida en la directiva.
   - Haga clic en el botón para denegar cambios en la configuración de tareas en equipos en red y autorizar la aplicación de la configuración de tareas establecida en la directiva.

   La directiva creada recientemente usa las configuraciones predeterminadas de las tareas de Protección del equipo en tiempo real.
   - Para modificar la configuración predeterminada de la tarea de Protección de archivos en tiempo real, haga clic en el botón **Configurar** en la subsección **Protección de archivos en tiempo real**. En la ventana que se abre, configure los privilegios de acceso según sus necesidades. Haga clic en **Aceptar**.
   - Para modificar la configuración predeterminada de la tarea de Uso de KSN, haga clic en el botón **Configurar** en la subsección **Uso de KSN**. En la ventana que se abre, configure los privilegios de acceso según sus necesidades. Haga clic en **Aceptar**.

     Para iniciar la tarea Uso de KSN, debe aceptar la Declaración de KSN en la ventana Manejo de datos (consulte la sección “Configuración de Manejo de datos mediante el complemento de administración”, en la página 276).
   - Para modificar la configuración predeterminada del componente Prevención de exploits, haga clic en el botón **Configurar** en la subsección **Prevención de exploits**. En la ventana que se abre, configure la funcionalidad según sus necesidades. Haga clic en **Aceptar**.
8. Seleccione uno de los siguientes estados de la directiva en la ventana **Crear la directiva de grupo para la aplicación**:
   - **Directiva activa**, si desea aplicar la directiva inmediatamente después de su creación. Si ya existe una directiva activa en el grupo, se desactiva y se aplica una directiva nueva.
   - **Directiva inactiva**, si no desea aplicar la directiva creada inmediatamente. En este caso, la directiva se puede activar más tarde.
   - Seleccione la casilla de verificación **Abrir propiedades de la directiva inmediatamente después de su creación** para cerrar automáticamente el **Asistente de nueva directiva** y configurar la directiva recién creada después de hacer clic en el botón **Siguiente**.
9. Haga clic en el botón **Finalizar**.

La directiva creada se mostrará en la lista de directivas de la pestaña **Directivas** del grupo de administración seleccionado. En la ventana **Propiedades: <Nombre de la directiva>**, puede establecer otra configuración, tareas y funciones de Kaspersky Embedded Systems Security.

Secciones de configuraciones de las directivas de Kaspersky Embedded Systems Security

General

En la sección **General**, puede configurar las siguientes opciones de la directiva:

- Especificar el estado de la directiva
- Configurar la herencia de las opciones de las directivas principales y las directivas secundarias.

Configuración de eventos

En la sección **Configuración de eventos**, puede configurar las opciones de las siguientes categorías de eventos:

- *Eventos críticos*
- *Fallo funcional*
- *Advertencia*
- *Mensaje Informativo*

Puede usar el botón **Propiedades** para configurar las siguientes opciones de los eventos seleccionados:

- Indicar la ubicación de almacenamiento y el periodo de retención de la información sobre los eventos registrados.
- Indicar el método de notificación de los eventos registrados.

Configuración de la aplicación

Tabla 11. Configuración de la sección Configuración de la aplicación

Sección	Opciones
Escalabilidad e interfaz	En la subsección **Escalabilidad e interfaz**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones: • Elija si desea ajustar la configuración de la escalabilidad automáticamente o manualmente. • Establecer la configuración de la visualización del icono de la aplicación
Seguridad	En la subsección **Seguridad**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones: • Establecer la configuración de ejecución de tareas • Especificar cómo debería comportarse la aplicación cuando el equipo se está ejecutando con energía de UPS • Habilitar o deshabilitar la protección con contraseña de funciones de la aplicación.
Conexiones	En la subsección **Conexiones**, puede usar el botón **Configurar** para configurar las siguientes opciones del servidor proxy para la conexión a KSN y a los servidores de actualizaciones y activación: • Configurar las opciones del servidor proxy • Especificar la configuración de autenticación del servidor proxy
Ejecutar tareas del sistema	En la subsección **Ejecutar tareas del sistema**, puede usar el botón **Configurar** para autorizar o bloquear el inicio de las siguientes tareas del sistema según la programación configurada en los equipos locales: • Tarea Análisis a pedido. • Tareas Actualización y Copia de actualizaciones.

Adicional

Tabla 12. Configuración de la sección Adicional

Sección	Opciones
Zona de confianza	Haga clic en el botón **Configurar** en la subsección **Zona de confianza** para configurar las siguientes opciones de la aplicación de la Zona de confianza: • Crear una lista de exclusiones de la Zona de confianza. • Habilitar o deshabilitar el análisis de las operaciones de copia de seguridad del archivo. • Crear una lista de procesos de confianza.
Análisis de unidades extraíbles	En la subsección **Análisis de unidades extraíbles**, puede usar el botón **Configurar** para configurar los parámetros de análisis para discos USB extraíbles.
Permisos de acceso de usuario para administrar la aplicación	En la subsección **Permisos de acceso de usuario para administrar la aplicación**, puede configurar los derechos del usuario y los derechos del grupo de usuarios para administrar Kaspersky Embedded Systems Security.
Permisos de acceso para administrar el servicio de Kaspersky Security	En la subsección **Permisos de acceso para administrar el servicio de Kaspersky Security**, puede configurar los derechos del usuario y los derechos del grupo de usuarios para administrar el servicio de Kaspersky Security.
Depósitos	En la sección **Depósitos**, haga clic en el botón **Configurar** para configurar las siguientes opciones de Cuarentena, Copia de seguridad y Hosts bloqueados: • Especificar la ruta de la carpeta en la cual desea colocar objetos en Cuarentena o Copia de seguridad. • Configurar el tamaño máximo de Copia de seguridad y Cuarentena y especificar el umbral de espacio disponible. • Especificar la ruta de la carpeta en la cual desea colocar objetos restaurados de la Cuarentena o la Copia de seguridad. • Configure el período de bloqueo del host.

Protección del equipo en tiempo real

Tabla 13. Configuración de la sección Protección del equipo en tiempo real

Sección	Opciones
Protección de archivos en tiempo real	En la subsección **Protección de archivos en tiempo real**, puede hacer clic en el botón **Configuración** para configurar las siguientes opciones de la tarea: • Indicar el modo de protección. • Configurar el uso del Analizador heurístico. • Configurar el uso de la Zona de confianza. • Indicar el alcance de la protección. • Configurar el nivel de seguridad para el alcance de la protección seleccionada: puede seleccionar un nivel de seguridad predefinido o establecer la configuración de la seguridad manualmente. • Configurar las opciones de inicio de tareas.

Sección	Opciones
Uso de KSN	En la subsección **Uso de KSN**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones de la tarea: • Indicar las acciones a realizar en objetos no confiables según KSN. • Configurar la transferencia de datos y el uso de Kaspersky Security Center como servidor KSN Proxy. Haga clic en el botón **Manejo de datos** para aceptar o rechazar la Declaración de KSN y de KMP, y configurar las opciones de intercambio de datos confiables.
Prevención de exploits	En la subsección **Prevención de exploits**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones de la tarea: • Seleccionar el modo de protección de memoria de proceso. • Indicar las acciones para reducir riesgos de exploits. • Añadir elementos a la lista de procesos protegidos y editar dicha lista.

Control de actividad local

Tabla 14. Configuración de la sección Control de actividad local

Sección	Opciones
Control de inicio de aplicaciones	En la subsección **Control de inicio de aplicaciones**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones de la tarea: • Seleccionar el modo de operación de tareas. • Configurar las opciones para controlar los inicios subsiguientes de la aplicación. • Indicar el área de la aplicación de las reglas de Control de inicio de aplicaciones. • Configurar el uso de KSN. • Configurar las opciones de inicio de tareas.
Control de dispositivos	En la subsección **Control de dispositivos**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones de la tarea: • Seleccionar el modo de operación de tareas. • Configurar las opciones de inicio de tareas.

Control de actividad de red

Tabla 15. Configuración de la sección Control de actividad de red

Sección	Opciones
Administración de firewall	En la subsección **Administración de firewall**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones de la tarea: • Configurar las reglas de firewall. • Configurar las opciones de inicio de tareas.

Inspección del sistema

Tabla 16. Configuración de la sección Inspección del sistema

Sección	Opciones
Monitor de integridad de archivos	En la subsección **Monitor de integridad de archivos**, puede configurar el control de los cambios en archivos que pueden significar una infracción de la seguridad en un equipo protegido.
Inspección de registros	En la sección **Inspección de registros**, puede configurar el control de integridad del equipo protegido sobre la base de los resultados del análisis de Registro de eventos de Windows.

Registros y notificaciones

Tabla 17. Configuración de la sección Registros y notificaciones

Sección	Opciones
Registros de tareas	En la subsección **Registros de tareas**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones: • Especificar el nivel de importancia de los eventos registrados para los componentes de la aplicación seleccionados. • Especificar la configuración de depósitos de almacenamiento del registro de tareas. • Especificar la integración de SIEM con la configuración de Kaspersky Security Center.
Notificaciones de eventos	En la subsección **Notificaciones de eventos**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones: • Especifique la configuración de la notificación del usuario para el evento *Objeto detectado*, el evento *Almacenamiento masivo dudoso detectado y restringido* y el evento *El host está en la lista de dudosos*. • Especificar la configuración de notificaciones del administrador para cualquier evento seleccionado en la lista de eventos en la sección **Configuración de notificaciones**.
Interacción con Servidor de administración	En la sección **Interacción con Servidor de administración**, puede hacer clic en el botón **Configurar** para seleccionar los tipos de objetos que Kaspersky Embedded Systems Security informará al Servidor de administración. También puede configurar la transmisión de información sobre los objetos en Cuarentena y Copia de seguridad al Servidor de administración.

Para revisar la información detallada acerca de las tareas de Protección de depósitos conectado en red, consulta la *Guía de implementación de Kaspersky Embedded Systems Security para la Protección de depósitos en red*.

Historial de revisiones

En la sección **Historial de revisiones**, puede administrar revisiones: compararlas con la revisión actual u otra directiva, agregue descripciones de revisiones, guardar revisiones de un archivo o realizar una reversión.

Configuración de directivas

En la ventana **Propiedades: <Nombre de la directiva>** de una directiva existente, puede establecer la configuración general de Kaspersky Embedded Systems Security, la configuración de la cuarentena y las copias de seguridad, la configuración de la Zona de confianza, la configuración de la Protección del equipo en tiempo real, la configuración del Control de actividad local, el nivel de detalle para los registros de tareas y las notificaciones de administrador y de usuario sobre eventos de Kaspersky Embedded Systems Security, los privilegios de acceso para administrar la aplicación y el servicio de Kaspersky Security, y la configuración de la aplicación del perfil de la directiva.

► *Para establecer la configuración de la directiva:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Expanda el grupo de administración, para el cual desea configurar las opciones de la directiva asociada y abra la pestaña **Directivas** en el panel de detalles.
3. Seleccione la directiva que desea configurar y abra la ventana **Propiedades: <Nombre de la directiva>** con uno de los siguientes métodos:
   - Seleccionando la opción **Propiedades** en el menú contextual de la directiva.
   - Haciendo clic en el vínculo **Configurar directiva** en el panel de detalles de la directiva seleccionada.
   - Haciendo doble clic en la directiva seleccionada.
4. En la pestaña **General** en la sección **Estado de la directiva**, habilite o deshabilite la directiva. Para esto, seleccione una de las siguientes opciones:
   - **Directiva activa**, si desea que la directiva se aplique en todos los equipos dentro del grupo de administración seleccionado.
   - **Directiva inactiva**, si desea activar la directiva más tarde en todos los equipos dentro del grupo de administración seleccionado.

   El parámetro **Directiva fuera de oficina** no está disponible cuando se administra Kaspersky Embedded Systems Security.
5. En las secciones **Configuración del evento**, **Configuración de la aplicación**, **Adicional**, **Registros y notificaciones** e **Historial de revisiones**, puede modificar la configuración de la aplicación (consulte la tabla a continuación).
6. En las secciones **Protección del equipo en tiempo real**, **Control de actividad local**, **Control de actividad de red** e **Inspección del sistema**, configure los parámetros de la aplicación y del inicio de la aplicación (consulte la tabla a continuación).

   Puede habilitar o deshabilitar la ejecución de cualquier tarea en todos los equipos dentro del grupo de administración mediante una directiva de Kaspersky Security Center.
   Puede configurar la aplicación de la configuración de la directiva en todos los equipos en red para cada componente de la aplicación particular.
7. Haga clic en **Aceptar**.

La configuración establecida se aplica en la directiva.

Creación y configuración de tareas con Kaspersky Security Center

Esta sección contiene información sobre las tareas de Kaspersky Embedded Systems Security y cómo crearlas, ajustar sus configuraciones, e iniciarlas y detenerlas.

En este capítulo

Acerca de la creación de tareas en Kaspersky Security Center

Puede crear tareas de grupo para grupos de administración y conjuntos de equipos. Puede crear los siguientes tipos de tareas:

- Activación de la aplicación
- Copia de actualizaciones
- Actualización de bases de datos
- Actualización de módulos del programa
- Reversión de la actualización de bases de datos
- Análisis a pedido
- Control de integridad de la aplicación
- Generador de reglas para Control de inicio de aplicaciones
- Generador de reglas para Control de dispositivos

Puede crear tareas de grupo y locales de las siguientes maneras:

- Para un equipo: en la ventana **Propiedades <Nombre del equipo>** en la sección **Tareas** .
- Para un grupo de administración: en el panel de detalles del nodo del grupo seleccionado de equipos en la pestaña **Tareas**.
- Para un conjunto de equipos: en el panel de detalles del nodo **Selecciones de dispositivos**.

Mediante el uso de directivas, puede deshabilitar programaciones de tareas del sistema local de actualizaciones y de Análisis a pedido (consulte la sección “Configuración del inicio programado de las tareas locales del sistema”, en la página 96) en todos los equipos protegidos desde el mismo grupo de administración.

Se proporciona información general sobre tareas en Kaspersky Security Center en la *Ayuda de Kaspersky Security Center*.

Creación de una tarea mediante Kaspersky Security Center

► *Para crear una tarea nueva en la Consola de administración de Kaspersky Security Center:*

1. Inicie el asistente de tareas de una de las siguientes maneras:
   - Para crear una tarea local:
     a. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo al cual pertenece el equipo protegido.
     b. En el panel de resultados, en la pestaña **Dispositivos**, abra el menú contextual del equipo protegido y seleccione **Propiedades**.
     c. En la ventana que se abre, haga clic en el botón **Agregar** en la sección **Tareas**.
   - Para crear una tarea de grupo:
     a. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
     b. Seleccione el grupo de administración para el cual desea crear una tarea.
     c. En el panel de detalles, abra la pestaña **Tareas** y seleccione **Crear una tarea**.
   - Para crear una tarea para un conjunto personalizado de equipos:
     a. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
     b. Seleccione el grupo de administración que contiene los equipos.
     c. Seleccione un equipo o un conjunto personalizado de equipos:
     d. En la lista desplegable **Realizar acción**, seleccione la opción **Crear una tarea**.

   Se abre la ventana del asistente de tareas.
2. En la ventana **Seleccionar el tipo de tarea**, en el encabezado **Kaspersky Embedded Systems Security**, seleccione el tipo de tarea que se creará.
3. Si selecciona cualquier tipo de tarea que no sea Reversión de la actualización de bases de datos, Control de integridad de la aplicación o Activación de la aplicación, se abrirá la ventana **Configuración**. Es posible que varíe la configuración según el tipo de tarea:
   - Cree una tarea de Análisis a pedido (consulte la sección “Creación de la tarea Análisis a pedido” en la página 409).
   - Para crear una tarea de actualización, configure los valores de la tarea según sus requisitos:
     a. Seleccione el origen de actualizaciones en la ventana **Origen de actualizaciones**.
     b. Haga clic en el botón **Configuración de conexión**. Se abrirá la ventana **Configuración de conexión**.
     c. En la ventana **Configuración de conexión**:

        Especifique el modo del servidor FTP para la conexión con el equipo protegido.

        Modifique el tiempo de espera de conexión al establecer conexión con el origen de actualizaciones, si es necesario.

        Defina la configuración de acceso al servidor proxy al establecer conexión con el origen de actualizaciones.

        Especifique la ubicación de los equipos protegidos con el fin de optimizar las descargas de actualizaciones.

- Para crear una tarea de Actualización de módulos del programa, configure los parámetros de actualización de los módulos del programa requeridos en la ventana **Configuración para la actualización de módulos del software de la aplicación**:

  a. Seleccione una de estas opciones para copiar e instalar actualizaciones del módulo del software críticas o solo comprobar su disponibilidad sin instalarlas.

  b. Si la opción **Copiar e instalar actualizaciones críticas de módulos del programa** está seleccionada: es posible que deba reiniciarse el equipo para aplicar los módulos de software instalados. Si desea que Kaspersky Embedded Systems Security reinicie el equipo automáticamente después de la finalización de la tarea, seleccione la casilla de verificación **Permitir el reinicio del sistema operativo**.

  c. Para obtener información sobre actualizaciones de módulos de Kaspersky Embedded Systems Security, seleccione **Informarme de las actualizaciones programadas que estén disponibles para los módulos del programa**.

  Kaspersky Lab no publica paquetes de actualizaciones planificadas en los servidores de actualizaciones para la instalación automática; se deben descargar manualmente desde el sitio web de Kaspersky Lab. Es posible configurar una notificación de administrador del evento **Está disponible una nueva actualización programada de módulos del programa**. Esto incluirá la URL de nuestro sitio web desde donde puede descargar las actualizaciones programadas.

- Para crear la tarea Copia de actualizaciones, especifique el conjunto de actualizaciones y la carpeta de destino en la ventana **Configuración de la copia de actualizaciones**.
- Para crear la tarea de Activación de la aplicación:

  a. En la ventana **Configuración de la activación**, especifique el archivo de clave que desea usar para activar la aplicación.

  b. Seleccione la casilla de verificación **Usar como clave adicional** si desea crear una tarea para renovar la licencia.

- Cree la tarea de Generador de reglas para Control de inicio de aplicaciones (consulte la sección “Creación de la tarea de Generador de reglas para Control de inicio de aplicaciones” en la página 313).
- Cree la tarea de Generador de reglas para Control de dispositivos (consulte la sección “Creación de la tarea de Generador de reglas para Control de dispositivos” en la página 352).

4. Configure la programación de la tarea (consulte la sección "Ajuste de configuración de la programación de inicio de tareas" en la página 128) (puede configurar una programación para todos los tipos de tarea excepto la tarea de Reversión de la actualización de bases de datos).
5. Haga clic en **Aceptar**.
6. Si la tarea creada es para un conjunto de equipos, seleccione los equipos (o el grupo) de red en los que se ejecutará esta tarea.
7. En la ventana **Seleccionar una cuenta para ejecutar la tarea**, especifique la cuenta con la cual desea ejecutar la tarea.
8. En la ventana **Especificar nombre de tarea**, especifique el nombre de la tarea (100 caracteres como máximo) que no contenga los símbolos **" * < > ? \ | :** .

   Se recomienda que el tipo de tarea se agregue a su nombre (por ejemplo, "Análisis a pedido de carpetas compartidas").
9. En la ventana **Finalizar creación de la tarea**, seleccione la casilla de verificación **Ejecutar tarea cuando el asistente finalice** si desea que la tarea se inicie tan pronto como se crea. Haga clic en el botón **Finalizar**.

La tarea creada se mostrará en la lista **Tareas**.

Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center

► *Para configurar tareas locales o la configuración general de la aplicación para un solo equipo de red:*

1. Amplíe el nodo **Dispositivos administrados** en el árbol del Servidor de administración de Kaspersky Security Center y seleccione el grupo al cual pertenece el equipo protegido.
2. En el panel de detalles, seleccione la pestaña **Dispositivos**.
3. Abra la ventana **Propiedades: <Nombre del equipo>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre del equipo protegido
   - Abra el menú contextual del nombre del equipo protegido y seleccione el elemento **Propiedades**

   Se abre la ventana **Propiedades:** Se abre la ventana **<Nombre del equipo>**.
4. Para configurar las opciones de la tarea local, siga estos pasos:
   a. Vaya a la sección **Tareas**.
      - En la lista de tareas, seleccione una tarea local para configurar.
      - Haga doble clic en el nombre de la tarea en la lista de tareas.
      - Seleccione el nombre de la tarea y haga clic en el botón **Propiedades**.
      - Seleccione **Propiedades** en el menú contextual de la tarea seleccionada.

        Se abre la ventana **Propiedades:** Se abre la ventana**<Nombre de la tarea>**.
5. Para configurar las opciones de la aplicación, siga estos pasos:
   a. Vaya a la sección **Aplicaciones**.
      - En la lista de aplicaciones instaladas, seleccione la aplicación que desea configurar.
      - Haga doble clic en el nombre de la aplicación en la lista de aplicaciones instaladas
      - Seleccione el nombre de la aplicación en la lista de aplicaciones instaladas y haga clic en el botón **Propiedades**.
      - Abra el menú contextual del nombre de la aplicación en la lista de aplicaciones instaladas y seleccione el elemento **Propiedades**.

        Se abrirá la ventana **Configuración de <Nombre de la aplicación>**.

> Si una aplicación está bajo una directiva de Kaspersky Security Center y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede editar a través de la ventana **Configuración de <Nombre de la aplicación>**.

Configuración de tareas de grupo en Kaspersky Security Center

► *Para configurar una tarea de grupo para varios equipos:*

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.
2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.
4. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.

   Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

5. Según el tipo de tarea configurada, realice una de las siguientes acciones:
   - Para configurar una tarea de Análisis a pedido:
     a. En la sección **área del análisis**, configure un área del análisis.
     b. En la sección **Opciones**, configure el nivel de prioridad de la tarea y la integración con otros componentes del programa.
   - Para configurar una tarea de actualización, establezca los valores de la tarea según sus requisitos:
     a. En la sección **Configuración**, establezca la configuración del origen de actualizaciones y la optimización de uso del subsistema del disco.
     b. Haga clic en el botón **Configuración de conexión** para configurar las opciones de conexión con el origen de actualizaciones.
   - Para configurar la tarea de Actualización de módulos del programa, en la sección **Configuración para la actualización de módulos del software de la aplicación**, elija una acción para realizar: copiar e instalar actualizaciones críticas de módulos de programa o solo comprobar si existen.
   - Para configurar la tarea Copia de actualizaciones, especifique el conjunto de actualizaciones y la carpeta de destino en la sección **Configuración de la copia de actualizaciones**.
   - Para configurar la tarea Activación de la aplicación, en la sección **Configuración de la activación**, aplique el archivo de clave que desea utilizar para activar la aplicación. Seleccione la casilla de verificación **Usar como clave adicional** si desea agregar un código de activación o archivo de clave para renovar la licencia.
   - Para configurar la generación automática de las reglas de autorización para el control del equipo, en la sección **Configuración**, especifique la configuración según la cual se creará la lista de reglas de autorización.
6. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación

para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).

7. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para la ejecución de la tarea. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.
8. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones del área de la tarea**. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.
9. En la ventana **Propiedades: <Nombre de la tarea>**, haga clic en **Aceptar**.

Se guardan las opciones de las tareas de grupo recientemente configuradas.

Los parámetros de tareas de grupo que están disponibles para la configuración se resumen en la tabla a continuación.

Tabla 18. Configuración de tareas de grupo de Kaspersky Embedded Systems Security

Tipos de tareas de Kaspersky Embedded Systems Security	Sección en la ventana Propiedades: <Nombre de la tarea>	Configuración de tareas
Generador de reglas para Control de inicio de aplicaciones	**Configuración**	Al configurar la tarea de Generador de reglas para Control de inicio de aplicaciones, puede hacer lo siguiente: • Crear reglas de autorización para las aplicaciones en ejecución; • Crear reglas de autorización para las aplicaciones de las carpetas específicas.
	Opciones	Puede especificar las acciones que desea realizar mientras crea reglas de autorización de Control de inicio de aplicaciones: • **Usar certificado digital** • **Usar sujeto y huella digital del certificado digital** • **De no haber un certificado, usar** • **Usar hash SHA256** • **Generar reglas para este usuario o grupo de usuarios** Puede establecer la configuración para archivos de configuración con listas de reglas de autorización que Kaspersky Embedded Systems Security crea después de la finalización de la tarea.
	Programación	Puede configurar las opciones del inicio programado de la tarea.

Tipos de tareas de Kaspersky Embedded Systems Security	Sección en la ventana Propiedades: <Nombre de la tarea>	Configuración de tareas
Generador de reglas para Control de dispositivos	**Configuración**	• Seleccione el modo de operación: considere los datos de sistema acerca de todos los dispositivos de almacenamiento masivo que se hayan conectado alguna vez o solo considere los depósitos masivos actualmente conectados. • Ajuste la configuración para archivos de configuración con listas de reglas de autorización que Kaspersky Embedded Systems Security crea después de la finalización de la tarea.
	Programación	Puede configurar las opciones del inicio programado de la tarea.
Activación de la aplicación (consulte la sección “Tarea Activación de la aplicación”, en la página 123)	**Configuración de la activación**	Para activar la aplicación o renovar la licencia, puede agregar un archivo de clave.
	Programación	Puede configurar las opciones del inicio programado de la tarea.
Copia de actualizaciones (consulte la sección “Tareas de actualización”, en la página 123)	**Origen de actualizaciones**	Puede especificar el Servidor de administración de Kaspersky Security Center o los servidores de actualizaciones de Kaspersky Lab como el origen de actualizaciones de la aplicación. También puede crear una lista personalizada de orígenes de actualizaciones: si agrega servidores FTP o HTTP personalizados o carpetas de red manualmente y los configura como orígenes de actualizaciones. Puede especificar el uso de Servidores de actualizaciones de Kaspersky Lab, si los servidores personalizados manualmente no están disponibles.
	Ventana **Configuración de conexión**	En la ventana **Configuración de conexiones** vinculada a la sección **Origen de actualizaciones**, puede especificar si debería establecerse la conexión con los servidores de actualizaciones de Kaspersky Lab o algún otro servidor mediante el servidor proxy.
	Configuración de la copia de actualizaciones	Puede especificar el conjunto de actualizaciones que desea copiar. En el campo **Carpeta de almacenamiento local para las actualizaciones copiadas**, especifique una ruta a una carpeta, que Kaspersky Embedded Systems Security utilizará para almacenar las actualizaciones copiadas.
	Programación	Puede configurar las opciones del inicio programado de la tarea.

Tipos de tareas de Kaspersky Embedded Systems Security	Sección en la ventana Propiedades: <Nombre de la tarea>	Configuración de tareas
Actualización de bases de datos (consulte la sección “Tareas de actualización”, en la página 123)	**Configuración**	Puede especificar el Servidor de administración de Kaspersky Security Center o los Servidores de actualizaciones de Kaspersky Lab como origen de actualizaciones de la aplicación en el cuadro de grupo **Origen de actualizaciones**. También puede crear una lista personalizada de orígenes de actualizaciones: si agrega servidores FTP o HTTP personalizados o carpetas de red manualmente y los configura como orígenes de actualizaciones. Puede especificar el uso de Servidores de actualizaciones de Kaspersky Lab, si los servidores personalizados manualmente no están disponibles. En la sección Optimización de lectura y escritura en disco, puede configurar la función que reduce la carga de trabajo en el subsistema del disco: • **Reducir la carga de lectura y escritura en disco** • **RAM usada para la optimización (MB)**
	Ventana **Configuración de conexión**	En la ventana **Configuración de conexiones** vinculada a la sección **Origen de actualizaciones**, puede especificar si debería establecerse la conexión con los servidores de actualizaciones de Kaspersky Lab o algún otro servidor mediante el servidor proxy.
	Programación	Puede configurar las opciones del inicio programado de la tarea.
Actualización de módulos del programa (consulte la sección “Tareas de actualización”, en la página 123)	**Origen de actualizaciones**	Puede especificar el Servidor de administración de Kaspersky Security Center o los servidores de actualizaciones de Kaspersky Lab como el origen de actualizaciones de la aplicación. También puede crear una lista personalizada de orígenes de actualizaciones: si agrega servidores FTP o HTTP personalizados o carpetas de red manualmente y los configura como orígenes de actualizaciones. Puede especificar el uso de Servidores de actualizaciones de Kaspersky Lab, si los servidores personalizados manualmente no están disponibles.
	Ventana **Configuración de conexión**	En el cuadro de grupo **Configuración de la conexión al origen de actualizaciones**, puede especificar si debería establecerse la conexión con los Servidores de actualizaciones de Kaspersky Lab o algún otro servidor mediante el servidor proxy.

Tipos de tareas de Kaspersky Embedded Systems Security	Sección en la ventana Propiedades: <Nombre de la tarea>	Configuración de tareas
	Configuración para la actualización de módulos del software de la aplicación	Puede especificar qué acciones debe realizar Kaspersky Embedded Systems Security cuando están disponibles o se hayan instalado actualizaciones críticas de los módulos de la aplicación, y también si Kaspersky Embedded Systems Security debe recibir información sobre las actualizaciones programadas.
	Programación	Puede configurar las opciones del inicio programado de la tarea.
Configuración del análisis a pedido (consulte la sección “Creación de la tarea Análisis a pedido” en la página 409)	**Área del análisis**	Puede especificar un área del análisis para la tarea de Análisis a pedido y configurar las opciones del nivel de seguridad.
	Ventana **Configuración del análisis a pedido**	En la ventana **Configuración del análisis a pedido** vinculada a la sección **Área del análisis**, puede seleccionar uno de niveles de seguridad predefinidos o personalizar el nivel de seguridad manualmente.
	Opciones	Puede activar o desactivar el uso del analizador heurístico para la tarea de Análisis a pedido y establecer el nivel de análisis mediante un control deslizante en el cuadro de grupo **Analizador heurístico**. En el cuadro de grupo **Integración con otros componentes**, puede configurar los siguientes componentes: • Aplicar la zona de confianza para tareas de Análisis a pedido. • Aplicar el Uso de KSN para las tareas de Análisis a pedido. • Configurar una prioridad para la tarea de Análisis a pedido: ejecutar tarea en segundo plano (prioridad baja) o considere la tarea de Análisis de áreas críticas.
	Programación	Puede configurar las opciones del inicio programado de la tarea.
Control de integridad de la aplicación (en la página 125)	**Programación**	Puede configurar las opciones del inicio programado de la tarea.

Para la tarea de Reversión de la actualización de bases de datos, puede establecer solo la configuración de la tarea estándar en las secciones **Notificación** y **Exclusiones del área de la tarea**, controladas por Kaspersky Security Center.

Para obtener información detallada sobre la configuración de opciones de estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

En esta sección

Activación de la tarea Aplicación

► *Para configurar la Activación de la tarea Aplicación, siga estos pasos:*

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.
2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.
4. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.

   Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.
5. En la sección **Configuración de la activación**, especifique el archivo de clave que desea usar para activar la aplicación. Seleccione la casilla de verificación **Usar como clave adicional** si desea agregar una clave para extender la licencia.
6. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
7. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para la ejecución de la tarea.
8. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones del área de la tarea**.

   Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.
9. En la ventana **Propiedades: <Nombre de la tarea>**, haga clic en **Aceptar**.

   Se guardan las opciones de las tareas de grupo recientemente configuradas.

Tareas de actualización

► *Para configurar las tareas Copia de actualizaciones, Actualización de bases de datos o Actualización*

de módulos del programa, haga lo siguiente:

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.
2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.
4. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.

   Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

5. Según el tipo de tarea configurada, realice una de las siguientes acciones:
   - En la sección **Origen de actualizaciones**, configure las opciones del origen de actualizaciones y la optimización de uso del subsistema del disco.
     a. Puede especificar el Servidor de administración de Kaspersky Security Center o los Servidores de actualizaciones de Kaspersky Lab como origen de actualizaciones de la aplicación en la sección **Origen de actualizaciones**. También puede crear una lista personalizada de orígenes de actualizaciones: si agrega servidores FTP o HTTP personalizados o carpetas de red manualmente y los configura como orígenes de actualizaciones.

        Puede especificar el uso de Servidores de actualizaciones de Kaspersky Lab, si los servidores personalizados manualmente no están disponibles.

     b. En la sección **Optimización de lectura y escritura en disco** de la tarea Actualización de bases de datos, puede configurar la función que reduce la carga de trabajo en el subsistema del disco:

        - **Reducir la carga de lectura y escritura en disco**

          Esta casilla de verificación habilita o deshabilita la función de optimización del subsistema del disco mediante el almacenamiento de archivos de actualización en una unidad virtual en la RAM.

          Si se activa la casilla, se habilita esta función.

          De forma predeterminada, la casilla está desactivada.

        - **RAM usada para la optimización (MB)**

          El tamaño de la RAM (en MB) que la aplicación usa para almacenar archivos de actualización. El tamaño de RAM predeterminado es 512 MB. El tamaño de RAM mínimo es 400 MB.

     c. Haga clic en el botón **Configuración de conexión** y, en la ventana **Configuración de conexión** que se abre, configure el uso de un servidor proxy para conectarse a servidores de actualizaciones de Kaspersky Lab y otros servidores.
   - En la **Configuración para la actualización de módulos del software de la aplicación** para la tarea Actualización de módulos del programa, puede especificar qué acciones debería realizar Kaspersky Embedded Systems Security cuando haya disponibles actualizaciones críticas del módulo del programa

o información sobre actualizaciones planificadas, y también puede especificar qué acciones debería realizar Kaspersky Embedded Systems Security durante la instalación de actualizaciones críticas.

- Especifique el conjunto de actualizaciones y la carpeta de destino en la sección **Configuración de la copia de actualizaciones** para la tarea Copia de actualizaciones.

6. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
7. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para la ejecución de la tarea.

> Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

8. En la ventana **Propiedades: <Nombre de la tarea>**, haga clic en **Aceptar**.

Se guardan las opciones de las tareas de grupo recientemente configuradas.

Para la tarea Reversión de la actualización de bases de datos, puede establecer solo la configuración de la tarea estándar controlada por Kaspersky Security Center en las secciones **Notificaciones** y **Exclusiones del área de la tarea**. Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

Control de integridad de la aplicación

► *Para configurar la tarea de grupo Control de integridad de la aplicación:*

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.
2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.
4. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.

> Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

5. En la sección **Dispositivos**, seleccione los dispositivos para los cuales desea configurar la tarea Control de integridad de la aplicación.
6. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
7. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para la ejecución de la tarea.

8. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones del área de la tarea**.

   Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

9. En la ventana **Propiedades: <Nombre de la tarea>**, haga clic en **Aceptar**.

   Se guardan las opciones de las tareas de grupo recientemente configuradas.

Configuración del diagnóstico de la interrupción en Kaspersky Security Center

Si ocurre un problema durante la operación de Kaspersky Embedded Systems Security (por ejemplo, Kaspersky Embedded Systems Security se interrumpe) y desea diagnosticarlo, puede habilitar la creación de archivos de seguimiento y el archivo de volcado del proceso de Kaspersky Embedded Systems Security, y enviar estos archivos para su análisis al Servicio de soporte técnico de Kaspersky Lab.

Kaspersky Embedded Systems Security no envía ningún archivo de volcado o rastreo automáticamente. Solo los usuarios con los permisos correspondientes pueden enviar datos de diagnóstico.

Kaspersky Embedded Systems Security escribe la información en los archivos de seguimiento y el archivo de volcado de memoria en formato no cifrado. El usuario selecciona la carpeta donde se guardan los archivos, que es administrada por la configuración del sistema operativo y la configuración de Kaspersky Embedded Systems Security. Puede configurar permisos de acceso (consulte la sección “Administración de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security” en la página 220) para permitir el acceso a registros, archivos de volcado y rastreo solo a usuarios requeridos.

► *Para configurar el diagnóstico de interrupciones en Kaspersky Security Center:*

1. En la Consola de administración de Kaspersky Security Center, abra la ventana **Configuración de la aplicación** (consulte la sección “**Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center**” en la página 117).
2. Abra la sección **Diagnóstico de mal funcionamiento** y realice lo siguiente:
   - Si desea que la aplicación escriba información de depuración en el archivo, seleccione la casilla de verificación **Escribir información de depuración en archivo de seguimiento**.
     - En el campo a continuación, especifique la carpeta en la cual Kaspersky Embedded Systems Security guardará los archivos de seguimiento.
     - Configure el nivel de detalle de la información de depuración.

       Esta lista desplegable le permite seleccionar el nivel de detalle de la información de depuración que Kaspersky Embedded Systems Security guarda en el archivo de seguimiento.

Puede seleccionar uno de los siguientes niveles de detalle:

- **Eventos críticos**: Kaspersky Embedded Systems Security guarda información únicamente sobre los eventos críticos en el archivo de rastreo.
- **Errores**: Kaspersky Embedded Systems Security guarda información sobre los eventos críticos y los errores en el archivo de rastreo.
- **Eventos importantes**: Kaspersky Embedded Systems Security guarda información sobre los eventos críticos, los errores y los eventos importantes en el archivo de seguimiento.
- **Eventos informativos**: Kaspersky Embedded Systems Security guarda información sobre los eventos críticos, los errores, los eventos importantes y los eventos informativos en el archivo de rastreo.
- **Toda la información de depuración**: Kaspersky Embedded Systems Security guarda toda la información de depuración en el archivo de rastreo.

Un representante de Soporte técnico determina el nivel de detalle que se debe establecer a fin de resolver el problema que surgió.

El nivel predeterminado de detalle está configurado como **Toda la información de depuración**.

La lista desplegable se encuentra disponible si está activada la casilla **Escribir información de depuración en archivo de seguimiento**.

- Especifique el tamaño máximo de los archivos de rastreo.
- Especifique los componentes que quiere depurar. Los códigos de componentes deben estar separados con punto y coma. Los códigos distinguen entre mayúsculas y minúsculas (consulte la tabla a continuación).

Tabla 19. Códigos del subsistema de Kaspersky Embedded Systems Security

Código del componente	Nombre del componente
*	Todos los componentes.
gui	Subsistema de la interfaz del usuario, complemento de Kaspersky Embedded Systems Security en Microsoft Management Console.
ak_conn	Subsistema para integrar el Agente de red y Kaspersky Security Center.
bl	Proceso de control, implementa tareas de control de Kaspersky Embedded Systems Security.
wp	Proceso de trabajo, administra las tareas de protección antivirus.
blgate	Proceso de administración remota de Kaspersky Embedded Systems Security.
ods	Subsistema del Análisis a pedido.
oas	Subsistema de Protección de archivos en tiempo real.
qb	Subsistema de cuarentena y Copia de seguridad.
scandll	Módulo auxiliar para análisis del antivirus.
core	Subsistema para la funcionalidad de antivirus básica.
avscan	Subsistema de procesamiento del antivirus.
avserv	Subsistema para controlar el núcleo del antivirus.

Código del componente	Nombre del componente
prague	Subsistema para la funcionalidad básica.
updater	Subsistema para actualizar los módulos del programa y las bases de datos.
snmp	Subsistema de soporte del protocolo SNMP.
perfcount	Subsistema del contador de rendimiento.

La configuración de rastreo del complemento de Kaspersky Embedded Systems Security (gui) y el Complemento de administración de Kaspersky Security Center (ak_conn) se aplica después de que se reinician estos componentes. La configuración de rastreo del subsistema de soporte del protocolo SNMP (snmp) se aplica después de que se reinicia el servicio SNMP. La configuración de rastreo del subsistema de contadores de rendimiento (perfcount) se aplica luego de que se reinician todos los procesos que usan contadores de rendimiento. La configuración de seguimiento para otros subsistemas de Kaspersky Embedded Systems Security se aplica tan pronto como se guarda la configuración del diagnóstico de la interrupción.

De forma predeterminada, Kaspersky Embedded Systems Security registra la información de depuración de todos los componentes de Kaspersky Embedded Systems Security.

El campo de entrada se encuentra disponible si está activada la casilla **Escribir información de depuración en archivo de seguimiento**.

- Si desea que la aplicación cree un archivo de volcado de memoria, seleccione la casilla de verificación **Crear archivo de volcado**.
  - En el campo a continuación, especifique la carpeta en la cual Kaspersky Embedded Systems Security guardará el archivo de volcado.

3. Haga clic en **Aceptar**.

La configuración de la aplicación establecida se aplica en el equipo protegido.

Administración de programaciones de tareas

Puede configurar la programación de inicio para tareas de Kaspersky Embedded Systems Security y establecer la configuración para ejecutar tareas según una programación.

En esta sección

Configuración de las opciones de programación de inicio de tareas

Puede configurar la programación de inicio de las tareas personalizadas y del sistema local en la Consola de la aplicación. No puede configurar la programación de inicio de tareas de grupo.

► *Para configurar las opciones de programación de inicio de tareas de grupo, siga estos pasos:*

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos**

administrados.

2. Seleccione el grupo al cual pertenece el servidor protegido.
3. En el panel de detalles, seleccione la pestaña **Tareas**.
4. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea.
   - Abra el menú contextual del nombre de la tarea y seleccione el elemento Propiedades
5. Seleccione la sección **Programación**.
6. En el bloque **Configuración de programación**, seleccione la casilla de verificación **Ejecutar según programación**.

   Los campos con la configuración de programación para la tarea Análisis a pedido y la tarea Actualización no estarán disponibles si el inicio programado está bloqueado por una directiva de Kaspersky Security Center.

7. Configure los valores de programación de acuerdo con sus requisitos. Para ello, realice las siguientes acciones:
   a. En la lista **Frecuencia**, seleccione uno de los siguientes valores:
      - **Horaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de horas; especifique el número de horas en el campo **Cada <número> hora(s)**.
      - **Diaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de días; especifique el número de horas en el campo **Cada <número> día(s)**.
      - **Semanal**, si desea que la tarea se ejecute con intervalos durante un número especificado de semanas; especifique el número de horas en el campo **Cada <número> semana(s)**. Especifique los días de la semana durante los cuales la tarea se iniciará (de manera predeterminada, las tareas se ejecutan los lunes).
      - **Al inicio de la aplicación**, si desea que la tarea se ejecute cada vez que se inicia Kaspersky Embedded Systems Security.
      - **Tras la actualización de bases de datos de la aplicación**, si desea que la tarea se ejecute después de cada actualización de bases de datos de la aplicación.
   b. Especifique la hora del primer inicio de la tarea en el campo **Hora de inicio**.
   c. En el campo **Fecha de inicio**, especifique la fecha desde la que se aplicará la programación.

      Después de especificar la frecuencia de inicio de la tarea, la hora del primer inicio de esta y la fecha desde la que se aplicará la programación, la información sobre la hora calculada para el próximo inicio de la tarea se mostrará en la parte superior de la ventana en el campo **Próximo inicio**. La información actualizada sobre la hora estimada del próximo inicio de la tarea se mostrará cada vez que abra la ventana **Configuración de tareas** de la pestaña **Programación**. El valor **Bloqueado por directiva** se muestra en el campo **Próximo inicio** si la configuración de la directiva activa de Kaspersky Security Center prohíbe el inicio de tareas programadas del sistema (consulte la sección “Configuración del inicio programado de las tareas locales del sistema”, en la página 96).

8. Use la pestaña **Avanzado** para configurar las siguientes opciones de programación de acuerdo con sus

requisitos.

- En la sección **Configuración de detención de la tarea**:
  a. Seleccione la casilla de verificación **Duración** y escriba el número requerido de horas y minutos en los campos a la derecha para especificar la duración máxima de la ejecución de la tarea.
  b. Seleccione la casilla de verificación **Pausar de** y escriba los valores de inicio y de finalización del intervalo de tiempo en los campos a la derecha para especificar el intervalo de tiempo inferior a 24 horas durante el cual la ejecución de la tarea se pausará.
- En la sección **Configuración avanzada**:
  a. Seleccione la casilla de verificación **Fin de la programación** y especifique la fecha desde la cual la programación dejará de funcionar.
  b. Seleccione la casilla de verificación **Ejecutar tareas omitidas** para habilitar el inicio de las tareas omitidas.
  c. Seleccione la casilla de verificación **Aleatorizar la hora de inicio de la tarea usando un margen de** y especifique el valor en minutos.

9. Haga clic en **Aceptar**.
10. Haga clic en el botón **Aplicar** para guardar la configuración del inicio de la tarea.

Si desea establecer la configuración de la aplicación para una sola tarea con Kaspersky Security Center, realice los pasos que se detallan en Configuración de tareas locales en la ventana de configuración de la aplicación de la sección Kaspersky Security Center (en la página 117).

Cómo habilitar y deshabilitar tareas programadas

Puede habilitar y deshabilitar tareas programadas antes o después de configurar las opciones de programación.

► *Para habilitar o deshabilitar la programación de inicio de tareas, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nombre de la tarea para la cual desea configurar la programación de inicio.
2. Seleccione **Propiedades**.

   Se abre la ventana **Configuración de tareas**.
3. En la ventana que se abre en la pestaña **Programación**, realice una de las siguientes acciones:
   - Seleccione la casilla de verificación **Ejecutar según programación** si desea habilitar el inicio programado de la tarea.
   - Cancela la selección de la casilla de verificación **Ejecutar según programación** si desea deshabilitar el inicio programado de la tarea.

     Las opciones de programación de inicio de tareas configuradas no se eliminan y se aplicarán en el siguiente inicio programado de la tarea.
4. Haga clic en **Aceptar**.
5. Haga clic en el botón **Aplicar**.

Se guardan las opciones de programación de inicio de tareas configuradas.

Informes en Kaspersky Security Center

Los informes en Kaspersky Security Center contienen información sobre el estado de dispositivos administrados. Los informes se basan en información almacenada en el Servidor de administración.

A partir de Kaspersky Security Center 11, los siguientes tipos de informes están disponibles para Kaspersky Embedded Systems Security:

- Informe sobre el estado de componentes de la aplicación
- Informe sobre aplicaciones prohibidas
- Informe sobre aplicaciones prohibidas en modo de prueba

Consulte la *Ayuda de Kaspersky Security Center* para obtener información detallada sobre todos los informes de Kaspersky Security Center y cómo configurarlos.

Informe sobre el estado de componentes de la aplicación

Puede supervisar el estado de protección de todos los dispositivos de red y acceder a un panorama estructurado del conjunto de componentes en cada dispositivo.

El informe muestra uno de los siguientes estados para cada componente: *En ejecución, En pausa, Detenido, Mal funcionamiento, No instalado, Iniciando*.

El estado *No instalado* hace referencia al componente, no a la aplicación. Si la aplicación no se instala, Kaspersky Security Center asigna el estado N/D (No disponible).

Puede crear selecciones de componentes y utilizar filtros para mostrar dispositivos de red con el conjunto definido de componentes y su estado.

Consulte la *Ayuda de Kaspersky Security Center* para acceder a información detallada sobre la creación y el uso de selecciones.

► *Para revisar los estados de componentes en la configuración de la aplicación:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. Seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).
3. Seleccione la sección **Componentes**.
4. Revise la tabla de estado.

► *Para revisar un informe estándar de Kaspersky Security Center:*

1. Seleccione el nodo **Servidor de administración <nombre del equipo>** en el árbol de la Consola de

administración.

2. Abra la pestaña **Informes**.
3. Haga doble clic en el elemento de la lista **Informe sobre el estado de los componentes de la aplicación**.

   Se genera un informe.
4. Revise los siguientes detalles del informe:
   - Un diagrama gráfico.
   - Una tabla con un resumen de los componentes y los números sumados de los dispositivos de red donde se instala cada uno de los componentes, y los grupos a los que pertenecen.
   - Una tabla detallada donde se especifica estado, versión, dispositivo y grupo del componente.

Informes sobre aplicaciones bloqueadas en los modos Activo y Solo estadísticas

En base a los resultados de la ejecución de la tarea Control de inicio de aplicaciones, pueden generarse dos tipos de informes: un informe sobre las aplicaciones prohibidas (si la tarea se inicia en el modo Activo) y un informe de las aplicaciones prohibidas en modo de prueba (si la tarea se inició en el modo Solo estadísticas). Estos informes muestran información sobre las aplicaciones bloqueadas en los equipos protegidos de la red. Cada informe se genera para todos los grupos de administración y acumula datos de todas las aplicaciones de Kaspersky Lab instaladas en los dispositivos protegidos.

► *Para revisar un informe sobre aplicaciones prohibidas en modo de prueba:*

1. Inicie la tarea Control de aplicaciones en el modo Solo estadísticas (consulte la sección “Configuración de la tarea Control de inicio de aplicaciones”, en la página 297).
2. Seleccione el nodo **Servidor de administración <nombre del equipo>** en el árbol de la Consola de administración.
3. Abra la pestaña **Informes**.
4. Haga doble clic en el elemento de la lista **Informe sobre aplicaciones prohibidas en modo de prueba**.

   Se genera un informe.
5. Revise los siguientes detalles del informe:
   - Un diagrama gráfico que muestra las diez primeras aplicaciones con la mayor cantidad de inicios bloqueados.
   - Una tabla que resume los bloques de aplicaciones ocurridos, donde se especifican el nombre del archivo ejecutable, el motivo, el tiempo de bloqueo y el número de dispositivos donde ocurrió.
   - Una tabla detallada donde se especifican datos sobre el dispositivo, la ruta de acceso del archivo y el criterio para el bloqueo.

► *Para revisar un informe sobre aplicaciones prohibidas en modo Activo:*

1. Inicie la tarea Control de aplicaciones en el modo Activo (consulte la sección “Configuración de la tarea Control de inicio de aplicaciones”, en la página 297).
2. Seleccione el nodo **Servidor de administración <nombre del equipo>** en el árbol de la Consola de administración.
3. Abra la pestaña **Informes**.

4. Haga doble clic en el elemento de la lista **Informe sobre aplicaciones prohibidas**.

   Se genera un informe.

Este informe consiste en los mismos bloques de datos que el informe sobre aplicaciones prohibidas en el modo de prueba.

Cómo usar la Consola de Kaspersky Embedded Systems Security

Esta sección proporciona información sobre la Consola de Kaspersky Embedded Systems Security y describe cómo administrar la aplicación mediante la Consola de la aplicación instalada en el equipo protegido o en otro equipo.

En este capítulo

Configuración de Kaspersky Embedded Systems Security en la Consola de la aplicación

La configuración general y la configuración del diagnóstico de mal funcionamiento de Kaspersky Embedded Systems Security establecen las condiciones generales para que la aplicación funcione. Este parámetro le permite controlar el número de procesos de trabajo que utiliza Kaspersky Embedded Systems Security, habilitar la recuperación de la tarea de Kaspersky Embedded Systems Security después de una cancelación anormal, mantener el registro de rastreo, habilitar la creación del archivo de volcado de los procesos de Kaspersky Embedded Systems Security en caso de una cancelación anormal y configurar otros parámetros generales.

Los ajustes de la aplicación no se pueden configurar en la Consola de la aplicación si la directiva activa de Kaspersky Security Center bloquea los cambios en estas opciones.

► *Para configurar Kaspersky Embedded Systems Security:*

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security** y realice una de las siguientes acciones:
   - Haga clic en el vínculo **Propiedades de la aplicación** en el panel de detalles del nodo.
   - Seleccione **Propiedades** en el menú contextual del nodo.

   Se abrirá la ventana **Configuración de la aplicación**.
2. En la ventana que se abre, configure las opciones generales de Kaspersky Embedded Systems Security de acuerdo con sus preferencias:
   - En la pestaña **Escalabilidad e interfaz**, se pueden configurar los valores siguientes:
     - En la sección **Configuración de escalabilidad**:
       - Número máximo de procesos de trabajo que puede ejecutar Kaspersky Embedded Systems Security

Tabla 20. Número máximo de procesos activos

<table>
<tr><th>Configuración</th><th>Número máximo de procesos activos</th></tr>
<tr><td>Descripción</td><td>Este parámetro pertenece al grupo Configuración de escalabilidad en Kaspersky Embedded Systems Security. Establece el número máximo de procesos activos que la aplicación puede ejecutar simultáneamente.
Aumentar el número de procesos que se ejecutan en paralelo aumenta la velocidad del análisis de archivos y mejora la seguridad contra errores de Kaspersky Embedded Systems Security. Sin embargo, si el valor de este parámetro es demasiado alto, puede reducir el rendimiento general del equipo y aumentar el uso de la RAM.
En la Consola de administración de la aplicación de Kaspersky Security Center, puede cambiar el parámetro Número máximo de procesos activos solo para Kaspersky Embedded Systems Security instalado en un equipo independiente (con el cuadro de diálogo Configuración de la aplicación); sin embargo, no puede modificar este parámetro en la configuración de directivas para grupos de equipos.</td></tr>
<tr><td>Valores posibles</td><td>1 a 8</td></tr>
<tr><td>Valor predeterminado</td><td>La aplicación gestiona la escalabilidad automáticamente según el número de procesadores en el equipo:
<table>
<tr><th>Número de procesadores</th><th>Número máximo de procesos activos</th></tr>
<tr><td>1</td><td>1</td></tr>
<tr><td>1< número de procesadores < 4</td><td>2</td></tr>
<tr><td>4 o más</td><td>4</td></tr>
</table></td></tr>
</table>

- Número de procesos para la protección del equipo en tiempo real

Tabla 21. Número de procesos para la protección en tiempo real

<table>
<tr><th>Configuración</th><th>Número de procesos para la protección en tiempo real</th></tr>
<tr><td>Descripción</td><td>Este parámetro pertenece al grupo Configuración de escalabilidad en Kaspersky Embedded Systems Security.
La utilización de este parámetro puede especificar el número fijo de procesos en los cuales Kaspersky Embedded Systems Security ejecutará tareas de Protección en tiempo real.
Un valor más alto de este parámetro aumentará la velocidad de análisis en las tareas de Protección en tiempo real. Sin embargo, cuantos más procesos use Kaspersky Embedded Systems Security, mayor será su influencia sobre el rendimiento general del equipo protegido y el uso de recursos de la RAM.
En la Consola de administración de la aplicación de Kaspersky Security Center, puede cambiar el parámetro Número de procesos para la protección en tiempo real solo para Kaspersky Embedded Systems Security instalado en un equipo independiente (con la ventana Configuración de la aplicación); sin embargo, no puede modificar este parámetro en la configuración de directivas para grupos de equipos.</td></tr>
<tr><td>Valores posibles</td><td>Valores posibles: 1-N, donde N es el valor especificado usando el parámetro Número máximo de procesos activos.
Si configura el valor del parámetro Número de procesos para la Protección en tiempo real como igual al número máximo de procesos activos, reducirá el impacto de Kaspersky Embedded Systems Security en la velocidad del intercambio de archivos entre los equipos y el equipo, lo que mejorará aún más su rendimiento durante la Protección en tiempo real. Sin embargo, las tareas de actualización y las tareas de Análisis a pedido con la prioridad básica Medio (Normal) se ejecutarán en procesos de Kaspersky Embedded Systems Security que ya se están ejecutando. Las tareas de Análisis a pedido se ejecutarán con menos velocidad. Si la ejecución de una tarea provoca la cancelación anormal de un proceso, se necesitará más tiempo para reiniciarlo.
Las tareas de Análisis a pedido con la prioridad básica Bajo siempre se ejecutan en un proceso o procesos independientes.</td></tr>
<tr><td>Valor predeterminado</td><td>Kaspersky Embedded Systems Security gestiona la escalabilidad automáticamente según el número de procesadores en el equipo:
<table>
<tr><th>Número de procesadores</th><th>Número de procesos para la protección en tiempo real</th></tr>
<tr><td>=1</td><td>1</td></tr>
<tr><td>>1</td><td>2</td></tr>
</table>
</td></tr>
</table>

- Número de procesos de trabajo para tareas de Análisis a pedido en segundo plano

Tabla 22. Número de procesos para tareas de Análisis a pedido en segundo plano

Configuración	Número de procesos para tareas de Análisis a pedido en segundo plano
Descripción	Este parámetro pertenece al grupo **Configuración de escalabilidad** en Kaspersky Embedded Systems Security. Puede usar este parámetro para especificar el número máximo de procesos que la aplicación utilizará para ejecutar las tareas de Análisis a pedido en el modo en segundo plano. El número de procesos especificados en este parámetro no se incluye en el número total de procesos de Kaspersky Embedded Systems Security especificados en el parámetro **Número máximo de procesos activos**. Por ejemplo, si especifica los valores de parámetros siguientes: • Número máximo de procesos activos: 3; • Número de procesos para las tareas de Protección en tiempo real: 3; • Número de procesos para tareas de Análisis a pedido en segundo plano: 1; y, luego, inicia tareas de Protección en tiempo real y una tarea de Análisis a pedido en el modo en segundo plano, el número total de procesos kavfswp.exe de Kaspersky Embedded Systems Security será 4. Es posible ejecutar varias tareas de Análisis a pedido en un proceso con prioridad baja. Puede aumentar el número de procesos, por ejemplo, si ejecuta varias tareas en el modo en segundo plano a fin de asignar un proceso independiente para cada tarea. La asignación de procesos independientes para tareas aumenta la confiabilidad y la velocidad de la ejecución de la tarea.
Valores posibles	1-4
Valor predeterminado	1

- En la sección **Interacción con el usuario**, seleccione si se mostrará el icono de la bandeja del sistema en la barra de tareas después del inicio de cada aplicación (consulte la sección “Icono de la bandeja del sistema en el área de notificación”, en la página 145).

- En la pestaña **Seguridad y fiabilidad**, se pueden configurar los valores siguientes:
  - En la sección **Configuración de confiabilidad**, especifique el número de intentos para recuperar

una tarea de Análisis a pedido después de que se haya interrumpido.

Tabla 23. Recuperación de tareas

Configuración	Recuperación de tareas (**Ejecutar recuperación de tarea**)
Descripción	Este parámetro pertenece al grupo **Configuración de confiabilidad** en Kaspersky Embedded Systems Security. Habilita la recuperación de tareas en caso de una cancelación de emergencia y define el número de intentos para recuperar tareas de Análisis a pedido. Cuando una tarea se interrumpe, el proceso kavfs.exe de Kaspersky Embedded Systems Security intenta reiniciar el proceso en el cual esa tarea se ejecutaba en el momento de la interrupción. Si la recuperación de la tarea está deshabilitada, la aplicación no restaura la Protección en tiempo real ni las tareas de Análisis a pedido. Si la recuperación de la tarea está habilitada, la aplicación intenta restaurar las tareas de Protección en tiempo real hasta que se inicien correctamente e intenta restaurar las tareas de Análisis a pedido usando el número de intentos especificados en el parámetro.
Valores posibles	Habilitado/deshabilitado. Número de intentos de recuperación de tareas de Análisis a pedido: 1 a 10.
Valor predeterminado	La recuperación de tareas está habilitada. Número de intentos de recuperación de tareas de Análisis a pedido: 2.

- En la sección **Acciones si se pasa a un sistema de alimentación de respaldo (UPS)**, especifique las acciones que realiza Kaspersky Embedded Systems Security después de cambiar a energía de UPS:

Tabla 24. Uso de un suministro de energía ininterrumpido

Configuración	Acciones si se pasa a un sistema de alimentación de respaldo (UPS).
Descripción	Este parámetro determina las acciones que Kaspersky Embedded Systems Security realiza cuando el equipo cambia a una fuente de suministro de energía ininterrumpida.
Valores posibles	Ejecute o no ejecute tareas de Análisis a pedido para que se inicien según una programación. Realice o detenga todas las tareas de Análisis a pedido activas.
Valor predeterminado	De forma predeterminada, si el equipo utiliza un suministro de energía ininterrumpida, Kaspersky Embedded Systems Security realiza lo siguiente: • No ejecuta tareas de Análisis a pedido que se ejecutan según la programación. • Detiene automáticamente todas las tareas de Análisis a pedido activas.

- En la sección **Ajustes de protección mediante contraseña**, configure las opciones de acceso protegido por contraseña de las funciones de la aplicación (consulte la sección “Acceso protegido con contraseña a las funciones de Kaspersky Embedded Systems Security” en la página 227).

- En la pestaña **Configuración de conexión**:
  - En la sección **Configuración del servidor proxy**, especifique la configuración de uso del servidor proxy.

- En la sección **Configuración de autenticación del servidor proxy**, especifique el tipo de autenticación y los detalles necesarios para la autenticación del servidor proxy.
- En la sección **Licencia**, especifique si Kaspersky Security Center se usará como un servidor proxy para la activación de la aplicación.

- En la pestaña **Diagnóstico de mal funcionamiento**:
  - Si desea que la aplicación escriba información de depuración en el archivo, seleccione la casilla de verificación **Escribir información de depuración en archivo de seguimiento**.
    - En el campo a continuación, especifique la carpeta en la cual Kaspersky Embedded Systems Security guardará los archivos de seguimiento.
    - Configure el nivel de detalle de la información de depuración.

      Esta lista desplegable le permite seleccionar el nivel de detalle de la información de depuración que Kaspersky Embedded Systems Security guarda en el archivo de seguimiento.

      Puede seleccionar uno de los siguientes niveles de detalle:

      - **Eventos críticos**: Kaspersky Embedded Systems Security guarda información únicamente sobre los eventos críticos en el archivo de rastreo.
      - **Errores**: Kaspersky Embedded Systems Security guarda información sobre los eventos críticos y los errores en el archivo de seguimiento.
      - **Eventos importantes**: Kaspersky Embedded Systems Security guarda información sobre los eventos críticos, los errores y los eventos importantes en el archivo de seguimiento.
      - **Eventos informativos**: Kaspersky Embedded Systems Security guarda información sobre los eventos críticos, los errores, los eventos importantes y los eventos informativos en el archivo de rastreo.
      - **Toda la información de depuración**: Kaspersky Embedded Systems Security guarda toda la información de depuración en el archivo de rastreo.

      Un representante de Soporte técnico determina el nivel de detalle que se debe establecer a fin de resolver el problema que surgió.

      El nivel predeterminado de detalle está configurado como **Toda la información de depuración**.

      La lista desplegable se encuentra disponible si está activada la casilla **Escribir información de depuración en archivo de seguimiento**.

    - Especifique el tamaño máximo de los archivos de rastreo.
    - Especifique los componentes que quiere depurar.

      Una lista de códigos de componentes de Kaspersky Embedded Systems Security para los cuales la aplicación guarda información de depuración en el archivo de seguimiento. Los códigos de componentes deben estar separados con punto y coma. Los códigos distinguen entre mayúsculas y minúsculas (consulte la tabla a continuación).

Tabla 25. Códigos del subsistema de Kaspersky Embedded Systems Security

Código del componente	Nombre del componente
*	Todos los componentes.

gui	Subsistema de la interfaz del usuario, complemento de Kaspersky Embedded Systems Security en Microsoft Management Console.
ak_conn	Subsistema para integrar el Agente de red y Kaspersky Security Center.
bl	Proceso de control, implementa tareas de control de Kaspersky Embedded Systems Security.
wp	Proceso de trabajo, administra las tareas de protección antivirus.
blgate	Proceso de administración remota de Kaspersky Embedded Systems Security.
ods	Subsistema del Análisis a pedido.
oas	Subsistema de Protección de archivos en tiempo real.
qb	Subsistema de cuarentena y Copia de seguridad.
scandll	Módulo auxiliar para análisis del antivirus.
core	Subsistema para la funcionalidad de antivirus básica.
avscan	Subsistema de procesamiento del antivirus.
avserv	Subsistema para controlar el núcleo del antivirus.
prague	Subsistema para la funcionalidad básica.
updater	Subsistema para actualizar los módulos del programa y las bases de datos.
snmp	Subsistema de soporte del protocolo SNMP.
perfcount	Subsistema del contador de rendimiento.

La configuración de seguimiento del complemento de Kaspersky Embedded Systems Security (gui) y el Complemento de administración de Kaspersky Embedded Systems Security para Kaspersky Security Center (ak_conn) se aplica después de que estos componentes se reinician. La configuración de rastreo del subsistema de soporte del protocolo SNMP (snmp) se aplica después de que se reinicia el servicio SNMP. La configuración de rastreo del subsistema de contadores de rendimiento (perfcount) se aplica luego de que se reinician todos los procesos que usan contadores de rendimiento. La configuración de seguimiento para otros subsistemas de Kaspersky Embedded Systems Security se aplica tan pronto como se guarda la configuración del diagnóstico de la interrupción.

De forma predeterminada, Kaspersky Embedded Systems Security registra la información de depuración de todos los componentes de Kaspersky Embedded Systems Security.

El campo de entrada se encuentra disponible si está activada la casilla **Escribir información de depuración en archivo de seguimiento**.

- Si desea que la aplicación cree un archivo de volcado de memoria, seleccione la casilla de verificación **Crear archivo de volcado de memoria**.

Kaspersky Embedded Systems Security no envía ningún archivo de volcado o rastreo automáticamente. Solo los usuarios con los permisos correspondientes pueden enviar datos de diagnóstico.

- En el campo a continuación, especifique la carpeta en la cual Kaspersky Embedded Systems

Security guardará el archivo de volcado de memoria.

Kaspersky Embedded Systems Security escribe la información en los archivos de seguimiento y los de volcado en formato no cifrado. El usuario selecciona la carpeta donde se guardan los archivos, que es administrada por la configuración del sistema operativo y la configuración de Kaspersky Embedded Systems Security. Puede configurar permisos de acceso (consulte la sección “Administración de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security” en la página 220) para permitir el acceso a registros, archivos de volcado y rastreo solo a usuarios requeridos.

1. Haga clic en **Aceptar**.

Se guarda la configuración de Kaspersky Embedded Systems Security.

Acerca de la Consola de Kaspersky Embedded Systems Security

La Consola de Kaspersky Embedded Systems Security es un complemento aislado agregado a Microsoft Management Console.

La aplicación se puede administrar mediante la Consola de la aplicación instalada en el equipo protegido o en cualquier otro equipo de la red corporativa.

Después de haber instalado la Consola de la aplicación en otro equipo, se requiere la configuración avanzada.

Si la Consola de la aplicación y Kaspersky Embedded Systems Security están instalados en equipos distintos asignados a dominios diferentes, es posible que se impongan limitaciones en cuento a la información que la aplicación brinda a la Consola de la aplicación. Por ejemplo, después de que se inicia cualquier tarea de la aplicación, su estado puede permanecer sin cambios en la Consola de la aplicación.

Durante la instalación de la Consola de la aplicación, el asistente de instalación crea el archivo kavfs.msc en la carpeta de instalación y agrega el complemento de Kaspersky Embedded Systems Security a la lista de complementos aislados de Microsoft Windows.

Puede iniciar la Consola de la aplicación en el menú **Inicio**. El archivo msc del complemento de Kaspersky Embedded Systems Security puede ejecutarse o agregarse a la instancia de Microsoft Management Console existente como un nuevo elemento en el árbol.

En una versión de 64 bits de Microsoft Windows, el complemento de Kaspersky Embedded Systems Security solo puede agregarse en la versión de 32 bits de Microsoft Management Console. Para hacerlo, abra Microsoft Management Console a través de la línea de comandos y ejecute el comando: mmc.exe /32.

Es posible agregar varios complementos de Kaspersky Embedded Systems Security a una Microsoft Management Console abierta en el modo de creación, a fin de usarla para administrar la protección de varios equipos en los que

está instalado Kaspersky Embedded Systems Security.

Desinstalación de interfaz de la Consola de Kaspersky Embedded Systems Security

La Consola de Kaspersky Embedded Systems Security se muestra en el árbol de Microsoft Management Console como un nodo.

Después de que se haya establecido la conexión con Kaspersky Embedded Systems Security instalado en un equipo diferente, el nombre del nodo se complementa con el nombre del equipo en el que se instaló la aplicación y el nombre de la cuenta de usuario con la que se estableció la conexión: **<Nombre del equipo> de Kaspersky Embedded Systems Security como <nombre de la cuenta>**. Después de la conexión con Kaspersky Embedded Systems Security instalado en el mismo equipo que la Consola de la aplicación, el nombre del nodo es **Kaspersky Embedded Systems Security**.

De forma predeterminada, la ventana de la Consola de la aplicación incluye los siguientes elementos:

- Árbol de la Consola de la aplicación
- Panel de detalles
- Barra de herramientas

El árbol de la Consola de la aplicación

El árbol de la Consola de la aplicación muestra el nodo **Kaspersky Embedded Systems Security** y los nodos secundarios de los componentes funcionales de la aplicación.

El nodo de **Kaspersky Embedded Systems Security** incluye los siguientes nodos secundarios:

- **Protección del equipo en tiempo real**: administra las tareas de protección en tiempo real y los servicios de KSN. El nodo **Protección del equipo en tiempo real** permite configurar las siguientes tareas:
  - **Protección de archivos en tiempo real**
  - **Uso de KSN**
- **Control del equipo**: controla los inicios de las aplicaciones instaladas en un equipo protegido, así como las conexiones de dispositivos externos. El nodo **Control del equipo** permite configurar las siguientes tareas:
  - **Control de inicio de aplicaciones**
  - **Control de dispositivos**
  - **Administración de firewall**
- **Generadores automatizados de reglas**: configuración de la generación automática de reglas del grupo y del sistema para las tareas Control de inicio de aplicaciones y Control de dispositivos.
  - **Generador de reglas para Control de inicio de aplicaciones**
  - **Generador de reglas para Control de dispositivos**
  - Tareas de grupo de generación de reglas **<Nombres de tareas>** (si corresponde)

Las tareas del grupo (consulte la sección “Categorías de tareas de Kaspersky Embedded Systems Security” en la página 147) se crean mediante Kaspersky Security Center. No puede administrar tareas de grupo a través de la Consola de la aplicación.

- **Inspección del sistema**: configuración del control de operaciones de archivos y configuración de inspección de registros de eventos de Windows.
  - **Monitor de integridad de archivos**
  - **Inspección de registros**
- **Análisis a pedido**: administra las tareas de análisis a pedido. Hay un nodo independiente para cada tarea:
  - **Análisis al inicio del sistema operativo**
  - **Análisis de áreas críticas**
  - **Análisis de archivos en cuarentena**
  - **Control de integridad de la aplicación**
  - Tareas personalizadas **<Nombres de la tarea>** (si corresponde)

  El nodo muestra tareas del sistema (consulte la sección “Categorías de tareas de Kaspersky Embedded Systems Security” en la página 147) que se crean cuando la aplicación se instala, tareas personalizadas y tareas de grupo de análisis a pedido creadas y enviadas a un equipo mediante Kaspersky Security Center.
- **Actualización**: administra las actualizaciones para los módulos y las bases de datos de Kaspersky Embedded Systems Security y copia las actualizaciones en la carpeta local de origen de actualizaciones. El nodo contiene nodos secundarios para administrar cada tarea de actualización y la tarea más reciente de Reversión de la actualización de bases de datos:
  - **Actualización de bases de datos**
  - **Actualización de módulos del programa**
  - **Copia de actualizaciones**
  - **Reversión de la actualización de bases de datos**

  El nodo muestra todas las tareas personalizadas y de actualización de grupo (consulte la sección “Categorías de tareas de Kaspersky Embedded Systems Security” en la página 147) creadas y enviadas a un equipo mediante Kaspersky Security Center.
- **Depósitos**: Administración de ajustes de Cuarentena y de Copia de seguridad.
  - **Cuarentena**
  - **Copia de seguridad**
- **Registros y notificaciones**: administra registros de tareas locales, el registro de seguridad y el registro de auditoría del sistema de Kaspersky Embedded Systems Security.
  - **Registro de seguridad**
  - **Registro de auditoría del sistema**
  - **Registros de tareas**
- **Licencia**: agregue o elimine claves y códigos de activación de Kaspersky Embedded Systems Security y consulte detalles de la licencia.

Panel de detalles

El panel de detalles muestra información sobre el nodo seleccionado. Si se selecciona el nodo **Kaspersky**

Embedded Systems Security, el panel de detalles muestra información sobre el estado de protección del equipo actual (consulte la sección “Ver estado de protección e información de Kaspersky Embedded Systems Security” en la página 158) e información sobre Kaspersky Embedded Systems Security, el estado de protección de sus componentes funcionales y la fecha de caducidad de la licencia.

Menú contextual del nodo Kaspersky Embedded Systems Security

Puede usar los elementos del menú contextual del nodo **Kaspersky Embedded Systems Security** para realizar las operaciones siguientes:

- **Conectarse a otro equipo**. Conectarse a otro equipo (consulte la sección “Administración de Kaspersky Embedded Systems Security mediante la Consola de la aplicación en otro equipo” en la página 146) para administrar las instancias de Kaspersky Embedded Systems Security instalados en él. También puede realizar esta operación si hace clic en el vínculo en la esquina inferior derecha del panel de detalles del nodo **Kaspersky Embedded Systems Security**.
- **Iniciar el servicio** / **Detener el servicio**. Iniciar o detener la aplicación o una tarea seleccionada (consulte la sección “Cómo iniciar/pausar/reanudar/detener tareas manualmente”, en la página 148). Para llevar a cabo estas operaciones, también puede usar los botones de la barra de herramientas. También puede realizar estas operaciones en los menús contextuales de tareas de la aplicación.
- **Configurar análisis de discos extraíbles**. Configure el análisis de unidades extraíbles (consulte la sección “Acerca de análisis de unidades extraíbles” en la página 403) conectadas al equipo protegido a través del puerto USB.
- **Prevención de exploits: ajustes generales**. Configure el modo de Prevención de exploits y establezca las acciones de prevención.
- **Prevención de exploits: configuración de protección de procesos**. Agregue procesos para la protección y seleccione las técnicas de prevención de exploits (consulte la sección "Técnicas de prevención de exploits" en la página 465).
- **Configurar los parámetros de Zona de confianza**. Consulte y configure las opciones de la Zona de confianza (consulte la sección “Acerca de la Zona de confianza” en la página 441).
- **Modificar los derechos de usuario de la administración de la aplicación**. Vea y configure los permisos de acceso a las funciones de Kaspersky Embedded Systems Security (consulte la sección “Administración de los permisos de acceso para administrar las funciones de Kaspersky Embedded Systems Security” en la página 220).
- **Modificar los derechos de usuario para administrar servicio de Kaspersky Security**. Vea y configure los derechos de usuario para administrar el servicio de Kaspersky Security (consulte la sección “Configuración de los permisos de acceso para administrar Kaspersky Embedded Systems Security y el servicio de Kaspersky Security” en la página 225).
- **Exportar configuración**. Guarde la configuración de la aplicación en un archivo de configuración con formato XML (consulte la sección “Exportación de configuración”, en la página 153). También puede realizar esta operación en los menús contextuales de las tareas de la aplicación.
- **Importar configuración**. Importe los parámetros de la aplicación desde un archivo de configuración con formato XML (consulte la sección “Importación de la configuración”, en la página 154). También puede realizar esta operación en los menús contextuales de las tareas de la aplicación.
- **Información acerca de la aplicación y las actualizaciones de módulos disponibles**. Consulte la información sobre Kaspersky Embedded Systems Security y las actualizaciones de módulos de la aplicación actualmente disponibles.
- **Actualizar**. Actualice el contenido de la ventana Consola de la aplicación. También puede realizar esta operación en los menús contextuales de las tareas de la aplicación.

- **Propiedades**. Consulte y configure Kaspersky Embedded Systems Security o una tarea seleccionada. También puede realizar esta operación en los menús contextuales de las tareas de la aplicación.

  Para hacerlo, también puede usar el vínculo **Propiedades de la aplicación** en el panel de detalles del nodo **Kaspersky Embedded Systems Security** o usar el botón en la barra de herramientas.

- **Ayuda**. Consulte información de la ayuda de Kaspersky Embedded Systems Security. También puede realizar esta operación en los menús contextuales de las tareas de la aplicación.

Barra de herramientas y menú contextual de las tareas de Kaspersky Embedded Systems Security

Puede administrar tareas de Kaspersky Embedded Systems Security con los elementos de los menús contextuales de cada tarea en el árbol de la Consola de la aplicación.

Puede usar los elementos del menú contextual para realizar las siguientes operaciones:

- **Iniciar**/**detener**. Inicie o detenga la ejecución de tareas (consulte la sección “Cómo iniciar/pausar/reanudar/detener tareas manualmente”, en la página 148). Para llevar a cabo estas operaciones, también puede usar los botones de la barra de herramientas.
- **Reanudar** / **Pausar**. Reanuda o pausa la ejecución de tareas (consulte la sección “Cómo iniciar/pausar/reanudar/detener tareas manualmente”, en la página 148). Para llevar a cabo estas operaciones, también puede usar los botones de la barra de herramientas. Esta operación está disponible para las tareas de Protección en tiempo real y Análisis a pedido.
- **Agregar tarea**. Cree una nueva tarea personalizada (consulte la sección “Creación y configuración de una tarea de Análisis a pedido” en la página 424). Esta operación está disponible para las tareas de Análisis a pedido.
- **Abrir registro**. Vea y administre un registro de tareas (consulte la sección “Acerca de los registros de tareas”, en la página 200). Esta operación está disponible para todas las tareas.
- **Eliminar tarea**. Elimine la tarea personalizada. Esta operación está disponible para las tareas de Análisis a pedido.
- **Plantillas de configuración**. Administre las plantillas (consulte la sección “Uso de plantillas de configuración de seguridad”, en la página 155). Esta operación está disponible para la Protección de archivos en tiempo real y Análisis a pedido.

Icono de la bandeja del sistema en el área de notificación

Cada vez que Kaspersky Embedded Systems Security se inicia automáticamente después de un reinicio del equipo, el icono de la bandeja del sistema se muestra en el área de notificación de la barra de tareas  Aparece de manera predeterminada si se instaló el componente del icono de la bandeja del sistema durante la instalación de la aplicación.

La apariencia del icono de la bandeja del sistema refleja el estado actual de la protección del equipo. Hay dos estados posibles:

 activo (icono en color) si al menos una de las siguientes tareas se está ejecutando actualmente: Protección de archivos en tiempo real, Control de inicio de aplicaciones

 inactivo (icono en blanco y negro) si ninguna de las siguientes tareas se está ejecutando actualmente: Protección de archivos en tiempo real, Control de inicio de aplicaciones

Para abrir el menú contextual del icono de la bandeja del sistema, haga clic sobre él con el botón derecho.

El menú contextual ofrece diversos comandos que se pueden utilizar para mostrar ventanas de aplicaciones (consulte la tabla a continuación).

Tabla 26. Comandos del menú contextual que se muestran en el icono de la bandeja del sistema

Comando	Descripción
Abrir la Consola de aplicaciones	Abre la Consola de Kaspersky Embedded Systems Security (si está instalada).
Abrir Interfaz de diagnóstico compacto	Abre la Interfaz de diagnóstico compacto.
Acerca de la aplicación	Abre la ventana Acerca de la aplicación que contiene información sobre Kaspersky Embedded Systems Security. Para los usuarios registrados de Kaspersky Embedded Systems Security, la ventana Acerca de la aplicación contiene información sobre las actualizaciones urgentes que se instalaron.
Ocultar	Oculta el icono de la bandeja del sistema en el área de notificación de la barra de herramientas.

Puede volver a ver el icono de la bandeja del sistema oculto en cualquier momento.

► *Para ver el icono de la aplicación de nuevo,*

en el menú **Inicio** de Microsoft Windows, seleccione **Todos los programas** > **Kaspersky Embedded Systems Security** > **Icono de la bandeja del sistema**.

Los nombres de configuración pueden variar en los diferentes sistemas operativos instalados.

En la configuración general de Kaspersky Embedded Systems Security, puede activar o desactivar la visualización del icono de la bandeja del sistema cada vez que la aplicación se inicia automáticamente después del reinicio del equipo.

Administración de Kaspersky Embedded Systems Security mediante la Consola de la aplicación en otro equipo

Puede administrar Kaspersky Embedded Systems Security mediante la Consola de la aplicación instalada en un equipo remoto.

Para administrar la aplicación con la Consola de Kaspersky Embedded Systems Security en un equipo remoto, asegúrese de lo siguiente:

- Los usuarios de la Consola de la aplicación en el equipo remoto se agregan al grupo de Administradores ESS en el equipo protegido.
- Las conexiones a la red se habilitan mediante el proceso del servicio de Kaspersky Security Management (kavfsgt.exe) si el firewall de Windows está habilitado en el equipo protegido.
- Durante la instalación de Kaspersky Embedded Systems Security, se seleccionó la casilla de verificación **Permitir el acceso remoto** en la ventana del Asistente de instalación.

Si Kaspersky Embedded Systems Security en el equipo remoto está protegido con contraseña, escríbala para obtener acceso a la administración de la aplicación mediante la Consola de la aplicación.

Administración de tareas de Kaspersky Embedded Systems Security

Esta sección contiene información sobre las tareas de Kaspersky Embedded Systems Security y cómo crearlas, ajustar sus configuraciones, e iniciarlas y detenerlas.

En esta sección

Categorías de tareas de Kaspersky Embedded Systems Security

Las funciones de Protección del equipo en tiempo real, Control del equipo, Análisis a pedido y Actualización en Kaspersky Embedded Systems Security se implementan como tareas.

Puede administrar tareas con el menú contextual de la tarea en el árbol de la Consola de la aplicación, la barra de herramientas y la barra de acceso rápido. Puede consultar información sobre el estado de la tarea en el panel de detalles. Las operaciones de administración de tareas se registran en el registro de auditoría del sistema.

Existen dos tipos de tareas de Kaspersky Embedded Systems Security: *locales* y *de grupo*.

Tareas locales

Las tareas locales solo se ejecutan en el equipo protegido para el que han sido creadas. Según el método de inicio, existen los siguientes tipos de tareas locales:

- **Tareas locales del sistema**. Se crean automáticamente durante la instalación de Kaspersky Embedded Systems Security. Puede modificar la configuración de todas las tareas del sistema, excepto las tareas del Análisis de archivos en cuarentena y de Reversión de la actualización de bases de datos. Las tareas del sistema no se pueden renombrar o eliminar. Puede ejecutar al mismo tiempo tareas de Análisis a pedido personalizadas y del sistema.
- **Tareas locales personalizadas**. En la Consola de la aplicación, puede crear tareas de Análisis a pedido. En Kaspersky Security Center, puede crear tareas de Análisis a pedido, Actualización de bases de datos, Reversión de la Actualización de bases de datos y Copia de actualizaciones. Tales tareas se denominan tareas personalizadas. Las tareas personalizadas se pueden renombrar, configurar y eliminar. Puede

ejecutar varias tareas personalizadas simultáneamente.

Tareas de grupo

Las tareas de grupo y las tareas para conjuntos de equipos creados mediante Kaspersky Security Center se muestran en la Consola de la aplicación. Tales tareas se denominan tareas de grupo. Las tareas de grupo pueden administrarse y configurarse desde Kaspersky Security Center. En la Consola de la aplicación, solo puede ver el estado de las tareas de grupo.

Cómo guardar una tarea después de modificar la configuración

Es posible modificar la configuración de una tarea que está en ejecución o detenida (en pausa). La configuración nueva se aplica según las siguientes condiciones:

- Si cambió la configuración de una tarea en ejecución, la configuración nueva se aplica inmediatamente después de guardar la tarea.
- Si cambió la configuración de una tarea detenida (pausada), la configuración nueva se aplica cuando la tarea se inicia la próxima vez.

► *Para guardar la configuración de la tarea modificada,*

en el menú contextual del nombre de la tarea, seleccione **Guardar tarea**.

Si después de modificar la configuración de la tarea, se selecciona otro nodo del árbol de la Consola de la aplicación primero el comando **Guardar tarea**, aparecerá la ventana para guardar la configuración.

► *Para guardar la configuración modificada al cambiar a otro nodo de la Consola de la aplicación,*

haga clic en **Sí** en la ventana guardar configuración.

Cómo iniciar, pausar, reanudar y detener tareas manualmente

Solo puede pausar y reanudar las tareas Protección del equipo en tiempo real y Análisis a pedido.

► *Para iniciar/pausar/reanudar/detener una tarea, siga estos pasos:*

1. Abra el menú contextual de la tarea en la Consola de la aplicación.
2. Seleccione una de las siguientes opciones: **Iniciar**, **Pausar**, **Reanudar** o **Detener**.

La operación se ejecuta y se registra en el registro de auditoría del sistema (en la página 198).

Cuando la tarea de Análisis a pedido se reanuda, Kaspersky Embedded Systems Security continúa con el objeto que se estaba analizando cuando la tarea se pausó.

Administración de programaciones de tareas

Puede configurar la programación de inicio para tareas de Kaspersky Embedded Systems Security y establecer la

configuración para ejecutar tareas según una programación.

En esta sección

Configuración de las opciones de programación de inicio de tareas

Puede configurar la programación de inicio de las tareas personalizadas y del sistema local en la Consola de la aplicación. No puede configurar la programación de inicio de tareas de grupo.

► *Para configurar las opciones de programación de inicio de tareas:*

1. Abra el menú contextual de la tarea para la que desea configurar la programación del inicio.
2. Seleccione **Propiedades**.

   Se abre la ventana **Configuración de tareas**.
3. En la ventana que se abre, en la pestaña **Programación**, seleccione la casilla de verificación **Ejecutar según programación**.
4. Configure los valores de programación de acuerdo con sus requisitos. Para ello, realice las siguientes acciones:
   a. En **Frecuencia**, seleccione uno de los siguientes valores:
      - **Horaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de horas; especifique el número de horas en el campo **Cada <número> hora(s)**.
      - **Diaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de días; especifique el número de horas en el campo **Cada <número> día(s)**.
      - **Semanal**, si desea que la tarea se ejecute con intervalos durante un número especificado de semanas; especifique el número de horas en el campo **Cada <número> semana(s)**. Especifique los días de la semana durante los cuales la tarea se iniciará (de manera predeterminada, las tareas se ejecutan los lunes).
      - **Al inicio de la aplicación**, si desea que la tarea se ejecute cada vez que se inicia Kaspersky Embedded Systems Security.
      - **Tras la actualización de bases de datos de la aplicación**, si desea que la tarea se ejecute después de cada actualización de bases de datos de la aplicación.
   b. Especifique la hora del primer inicio de la tarea en el campo **Hora de inicio**.
   c. En el campo **Fecha de inicio**, especifique la fecha desde la que se aplicará la programación.

   Después de especificar la frecuencia de inicio de la tarea, la hora del primer inicio de esta y la fecha desde la que se aplicará la programación, la información sobre la hora calculada para el próximo inicio de la tarea se mostrará en la parte superior de la ventana en el campo **Próximo inicio**. La información actualizada sobre la hora estimada del próximo inicio de la tarea se mostrará cada vez que abra la ventana **Configuración de tareas** de la pestaña **Programación**.

El campo **Bloqueado por directiva** se muestra en el campo **Próximo inicio** si las tareas de inicio del sistema en una programación están configuradas en las opciones de la directiva de Kaspersky Security Center.

5. Use la pestaña **Avanzado** para configurar las siguientes opciones de programación de acuerdo con sus requisitos.
   - En la sección **Configuración de detención de la tarea**:
     a. Seleccione la casilla de verificación **Duración** y escriba el número requerido de horas y minutos en los campos a la derecha para especificar la duración máxima de la ejecución de la tarea.
     b. Seleccione la casilla de verificación **Pausar de** y escriba los valores de inicio y de finalización del intervalo de tiempo en los campos a la derecha para especificar el intervalo de tiempo inferior a 24 horas durante el cual la ejecución de la tarea se pausará.
   - En la sección **Configuración avanzada**:
     a. Seleccione la casilla de verificación **Fin de la programación** y especifique la fecha desde la cual la programación dejará de funcionar.
     b. Seleccione la casilla de verificación **Ejecutar tareas omitidas** para habilitar el inicio de las tareas omitidas.
     c. Seleccione la casilla de verificación **Aleatorizar el inicio de la tarea usando un margen de** y especifique el valor en minutos.
6. Haga clic en **Aceptar**.

Se guarda la configuración de inicio de la tarea.

Cómo habilitar y deshabilitar tareas programadas

Puede habilitar y deshabilitar tareas programadas antes o después de configurar las opciones de programación.

► *Para habilitar o deshabilitar la programación de inicio de tareas, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nombre de la tarea para la cual desea configurar la programación de inicio.
2. Seleccione **Propiedades**.

   Se abre la ventana **Configuración de tareas**.
3. En la ventana que se abre en la pestaña Programación, realice una de las siguientes acciones:
   - Seleccione la casilla de verificación **Ejecutar según programación** si desea habilitar el inicio programado de la tarea.
   - Cancela la selección de la casilla de verificación **Ejecutar según programación** si desea deshabilitar el inicio programado de la tarea.

     Las opciones de programación de inicio de tareas configuradas no se eliminan y se aplicarán en el siguiente inicio programado de la tarea.
4. Haga clic en **Aceptar**.

Se guardan las opciones de programación de inicio de tareas configuradas.

Uso de cuentas de usuario para iniciar tareas

Puede iniciar tareas con la cuenta de sistema o bien especificar una cuenta diferente.

En esta sección

Acerca del uso de cuentas para iniciar tareas

Puede especificar la cuenta con la cual desea ejecutar la tarea seleccionada para los siguientes componentes funcionales de Kaspersky Embedded Systems Security:

- Tareas del Generador de reglas para Control de inicio de aplicaciones y Generador de reglas para Control de dispositivos
- Tarea Análisis a pedido
- Tareas de actualización

De forma predeterminada, estas taras se ejecutan según los permisos de la cuenta de sistema.

Se recomienda especificar una cuenta diferente con los permisos de acceso adecuados en los siguientes casos:

- En la tarea Actualizar, si especificó la carpeta pública en un equipo distinto de la red como el origen de actualizaciones.
- En la tarea Actualizar, si un servidor proxy con autenticación NTLM de Windows incorporada se usa para acceder al origen de actualizaciones.
- En las tareas de Análisis a pedido, si la cuenta de sistema no posee permisos para acceder a ninguno de los objetos analizados (por ejemplo, a archivos en carpetas compartidas en el equipo).
- En la tarea de Generador de reglas para Control de inicio de aplicaciones, si, después de que la tarea finalice, las reglas generadas se exportan a un archivo de configuración ubicado en una ruta a la cual la cuenta de sistema no puede acceder (por ejemplo, en una de las carpetas compartidas en el equipo).

Puede ejecutar tareas de Actualización, Análisis a pedido y Generador de reglas con permisos de la cuenta de sistema. Durante la ejecución de estas tareas, Kaspersky Embedded Systems Security accede a las carpetas compartidas en otro equipo en la red si este equipo está registrado en el mismo dominio que el equipo protegido. En este caso, la cuenta de sistema debe poseer permisos de acceso a estas carpetas. Kaspersky Embedded Systems Security accederá al equipo con permisos de la cuenta **<nombre de dominio\nombre_del_equipo>**.

Especificación de una cuenta de usuario para iniciar una tarea

► *Para especificar una cuenta para el inicio de una tarea, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nombre de la tarea para la cual

desea configurar el inicio con permisos de la cuenta.

2. Seleccione **Propiedades**.

   Se abre la ventana **Configuración de tareas**.

3. En la ventana que se abre, haga lo siguiente en la pestaña **Ejecutar como**:

   a. Seleccione **Nombre de usuario**.

   b. Escriba el nombre de usuario y la contraseña de la cuenta que desea usar.

   > El usuario seleccionado debe estar registrado en el equipo protegido o en el mismo dominio que este equipo.

   c. Confirme la contraseña que se introdujo.

4. Haga clic en **Aceptar**.

Se guarda la configuración modificada para ejecutar la tarea con permisos de la cuenta de usuario.

Cómo importar y exportar la configuración

Esta sección brinda información sobre cómo exportar la configuración de Kaspersky Embedded Systems Security o la configuración de componentes de la aplicación específicos a un archivo de configuración en formato XML y cómo importar dicha configuración desde ese archivo de configuración de nuevo a la aplicación.

En esta sección

Acerca de la importación y exportación de la configuración

Puede exportar la configuración de Kaspersky Embedded Systems Security a un archivo de configuración XML e importar los parámetros a Kaspersky Embedded Systems Security desde el archivo de configuración. Puede guardar todos los ajustes de la aplicación o únicamente los ajustes de componentes individuales a un archivo de configuración.

Cuando exporta toda la configuración de Kaspersky Embedded Systems Security a un archivo, se guarda la configuración de la aplicación general y la configuración de los siguientes componentes y funciones de Kaspersky Embedded Systems Security:

- Protección de archivos en tiempo real
- Uso de KSN
- Control de dispositivos
- Control de inicio de aplicaciones
- Generador de reglas para Control de dispositivos
- Generador de reglas para Control de inicio de aplicaciones

- Tareas de Análisis a pedido
- Monitor de integridad de archivos
- Inspector del registro
- Base de datos y actualización de módulos del programa de Kaspersky Embedded Systems Security
- Cuarentena
- Copia de seguridad
- Registros.
- Notificaciones de administrador y usuario
- Zona de confianza
- Prevención de exploits
- Protección con contraseña

Además, se puede guardar la configuración general de Kaspersky Embedded Systems Security en el archivo, así como los derechos de las cuentas de usuario.

No puede exportar la configuración de tareas de grupo.

Kaspersky Embedded Systems Security exporta todas las contraseñas usadas por la aplicación, por ejemplo, los datos de la cuenta para ejecutar tareas o conectarse a un servidor proxy. Las contraseñas exportadas se guardan en forma cifrada en el archivo de configuración. Puede importar contraseñas solo usando Kaspersky Embedded Systems Security instalado en este equipo si no se ha instalado de nuevo ni se ha actualizado.

No puede importar contraseñas guardadas anteriormente con Kaspersky Embedded Systems Security instalado en un equipo diferente. Después de haber importado la configuración a otro equipo, todas las contraseñas se deben introducir en forma manual.

Si una directiva de Kaspersky Security Center está activa en el momento de la exportación, la aplicación exporta los valores especificados usados por esa directiva.

Se pueden importar parámetros de un archivo de configuración que contiene parámetros para componentes individuales de Kaspersky Embedded Systems Security (por ejemplo, de un archivo creado en la aplicación Kaspersky Embedded Systems Security instalado con un conjunto incompleto de componentes). Después de la importación de la configuración, solo se modifican los parámetros de Kaspersky Embedded Systems Security incluidos en el archivo de configuración. Todos los demás parámetros permanecen iguales.

La configuración de una directiva activa de Kaspersky Security Center que se ha bloqueado no cambia al importar la configuración.

Exportación de la configuración

► *Para exportar configuraciones a un archivo de configuración, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, realice una de las siguientes acciones:
   - En el menú contextual del nodo **Kaspersky Embedded Systems Security**, seleccione **Exportar configuración** para exportar toda la configuración de Kaspersky Embedded Systems Security.
   - En el menú contextual de la tarea cuya configuración desea exportar, seleccione **Exportar configuración** para exportar la configuración de un componente funcional individual de la aplicación.

- Para exportar la configuración del componente de la zona de confianza:
  a. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security**.
  b. Seleccione **Configurar los parámetros de Zona de confianza**.

     Se abre la ventana **Zona de confianza**.
  c. Haga clic en el botón **Exportar**.

     La ventana de bienvenida del asistente para la exportación de la configuración se abre.

2. Siga las instrucciones en el **Asistente**: especifique el nombre del archivo de configuración para guardar la configuración y la ruta de acceso a esta.

   Se pueden usar variables del entorno del sistema al especificar la ruta; no se permiten variables del entorno del usuario.

   > Si una directiva de Kaspersky Security Center está activa en el momento de la exportación, la aplicación exporta los valores de la configuración usados por esa directiva.

3. Haga clic en el botón **Cerrar** en la ventana **Finalizó la exportación de la configuración de la aplicación**.

La configuración de exportación se guarda cuando el asistente se cierra.

Importación de la configuración

► *Para importar configuraciones de un archivo de configuración guardado, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, realice una de las siguientes acciones:
   - En el menú contextual del nodo **Kaspersky Embedded Systems Security**, seleccione **Importar configuración** para importar todos los parámetros de Kaspersky Embedded Systems Security.
   - En el menú contextual de la tarea cuya configuración desea exportar, seleccione **Importar configuración** para importar la configuración de un componente funcional individual de la aplicación.
   - Para importar la configuración del componente de la zona de confianza:
     a. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security**.
     b. Seleccione **Configurar los parámetros de Zona de confianza**.

        Se abre la ventana **Zona de confianza**.
     c. Haga clic en el botón **Importar**.

        La ventana de bienvenida del asistente para la importación de la configuración se abre.
2. Siga las instrucciones del asistente: especifique el archivo de configuración desde el que desea importar parámetros.

   > Después de haber importado la configuración general de Kaspersky Embedded Systems Security o sus componentes funcionales en el equipo, no podrá volver a los valores de configuración anteriores.

3. Haga clic en el botón **Cerrar** en la ventana **Finalizó la importación de la configuración de la aplicación**.

   La configuración importada se guardará cuando el asistente se cierre.
4. En la barra de herramientas de la Consola de la aplicación, haga clic en el botón **Actualizar**.

La configuración importada se muestra en la ventana Consola de la aplicación.

Kaspersky Embedded Systems Security no importa contraseñas (datos de la cuenta utilizada para iniciar tareas o establecer conexión con el servidor proxy) del archivo creado en otro equipo o en el mismo equipo después de que Kaspersky Embedded Systems Security se haya reinstalado o actualizado. Después de finalizar la operación de importación, las contraseñas deben especificarse manualmente.

Uso de plantillas de configuración de seguridad

Esta sección contiene información sobre el uso de las plantillas de configuración de seguridad en las tareas de análisis y protección de Kaspersky Embedded Systems Security.

En esta sección

Acerca de las plantillas de configuración de seguridad

Puede configurar manualmente los ajustes de seguridad de un nodo en el árbol o en una lista de recursos del archivo del equipo y guardar los valores de ajuste configurados como plantilla. Esta plantilla se puede utilizar entonces para configurar las opciones de seguridad de otros nodos en las tareas de análisis y protección de Kaspersky Embedded Systems Security.

Las plantillas pueden utilizarse para configurar las opciones de seguridad de las siguientes tareas de Kaspersky Embedded Systems Security:

- Protección de archivos en tiempo real
- Análisis al inicio del sistema operativo
- Análisis de áreas críticas
- Tareas de Análisis a pedido

La configuración de seguridad de una plantilla aplicada a un nodo principal en el árbol de recursos de archivos del equipo se aplica en todos los nodos secundarios. La plantilla de un nodo principal no se aplica a nodos secundarios en los casos siguientes:

- Si la configuración de seguridad de los nodos secundarios se establece por separado (consulte la sección “Aplicación de una plantilla de configuración de seguridad”, en la página 156).
- Si los nodos secundarios son virtuales. Debe aplicar la plantilla a cada nodo virtual por separado.

Creación de una plantilla de configuración de seguridad

► *Para guardar manualmente la configuración de seguridad de un nodo y guardar esa configuración en una plantilla:*

1. En el árbol de la Consola de la aplicación, seleccione la tarea para la cual desea aplicar la plantilla de configuración de seguridad.
2. En el panel de detalles de la tarea seleccionada, haga clic en el vínculo **Configurar el área de protección** o **Configurar el área de análisis**.
3. En el árbol o en la lista de recursos de archivos en red del equipo, seleccione la plantilla que desea visualizar.
4. En la pestaña **Nivel de seguridad**, haga clic en el botón **Guardar como plantilla**.

   Se abre la ventana **Propiedades de la plantilla**.
5. En el campo **Nombre de la plantilla**, ingrese el nombre de la plantilla.
6. Escriba información adicional sobre la plantilla en el campo **Descripción**.
7. Haga clic en **Aceptar**.

Se guardará la plantilla con el conjunto de configuraciones de seguridad.

Visualización de la configuración de seguridad en una plantilla

► *Para visualizar la configuración de seguridad en una plantilla que creó, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, seleccione la tarea para la cual desea ver la plantilla de seguridad.
2. En el menú contextual de la tarea seleccionada, seleccione **Plantillas de configuración**.

   Se abre la ventana **Plantillas**.
3. En la lista de plantillas en la ventana que se abre, seleccione la plantilla que desea ver.
4. Haga clic en el botón **Ver**.

Se abre la ventana **<Nombre de la plantilla>**. La pestaña **General** muestra el nombre de la plantilla e información adicional sobre la plantilla; la pestaña **Opciones** enumera los valores de configuración de seguridad guardados en la plantilla.

Aplicación de una plantilla de configuración de seguridad

► *Para aplicar la configuración de seguridad de una plantilla a un nodo seleccionado:*

1. En el árbol de la Consola de la aplicación, seleccione la tarea para la cual desea aplicar la plantilla de configuración de seguridad.
2. En el panel de detalles de la tarea seleccionada, haga clic en el vínculo **Configurar el área de protección** o **Configurar el área de análisis**.
3. En el árbol o en la lista de recursos de archivos en red del equipo, abra el menú contextual del nodo o del elemento al cual desea aplicar la plantilla.
4. Seleccione **Aplicar plantilla** → **<Nombre de la plantilla>**.

5. Haga clic en el botón **Guardar**.

La plantilla de configuración de seguridad se aplica al nodo seleccionado en el árbol de los recursos del archivo del equipo. La pestaña **Nivel de seguridad** del nodo seleccionado ahora tiene el valor **Personalizado**.

La configuración de seguridad de una plantilla aplicada a un nodo principal en el árbol de recursos de archivos del equipo se aplica en todos los nodos secundarios.

Si el alcance de la protección o el área del análisis de los nodos secundarios en el árbol de recursos de archivos del equipo se configuraron por separado, la configuración de seguridad de la plantilla aplicada al nodo principal no se aplica automáticamente a tales nodos secundarios.

► *Para aplicar la configuración de seguridad de una plantilla a todos los nodos seleccionados, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, seleccione la tarea para la cual desea aplicar la plantilla de configuración de seguridad.
2. En el panel de detalles de la tarea seleccionada, haga clic en el vínculo **Configurar el área de protección** o **Configurar el área de análisis**.
3. En el árbol o en la lista de recursos de archivos en red del equipo, seleccione un nodo principal para aplicar la plantilla al nodo seleccionado y a todos los nodos secundarios.
4. En el menú contextual, seleccione **Aplicar plantilla → <Nombre de la plantilla>**.
5. Haga clic en el botón **Guardar**.

La plantilla de configuración de seguridad se aplica a los nodos principales y a todos los nodos secundarios en el árbol de recursos de archivos del equipo. La pestaña **Nivel de seguridad** del nodo seleccionado ahora tiene el valor **Personalizado**.

Eliminación de una plantilla de configuración de seguridad

► *Para eliminar una plantilla de configuración de seguridad, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, seleccione la tarea para cuya configuración ya no desea usar una plantilla de configuración de seguridad.
2. En el menú contextual de la tarea seleccionada, seleccione **Plantillas de configuración**.

   Puede consultar plantillas de configuración para las tareas de Análisis a pedido desde el panel de detalles del nodo principal **Análisis a pedido**.

   Se abre la ventana **Plantillas**.
3. En la lista de plantillas en la ventana que se abre, seleccione la plantilla que desea eliminar.
4. Haga clic en el botón **Eliminar**.

Una ventana se abre para confirmar la eliminación.

5. En la ventana que se abre, haga clic en **Sí**.

La plantilla seleccionada se elimina.

Si la plantilla de configuración de seguridad se aplicó para proteger o analizar nodos de recursos de archivos del equipo, la configuración de seguridad para tales nodos se conserva después de que la plantilla se elimina.

Consultar el estado de protección e información de Kaspersky Embedded Systems Security

► *Para consultar información sobre el estado de protección del equipo de Kaspersky Embedded Systems Security,*

seleccione el nodo **Kaspersky Embedded Systems Security** en el árbol de la Consola de la aplicación.

De forma predeterminada, la información en el panel de detalles de la Consola de la aplicación se actualiza automáticamente:

- Cada 10 segundos en caso de una conexión local.
- Cada 15 segundos en caso de una conexión remota.

Se puede actualizar la información de forma manual.

► *Para actualizar la información del nodo **Kaspersky Embedded Systems Security** de forma manual,*

seleccione el comando **Actualizar** en el menú contextual del nodo **Kaspersky Embedded Systems Security**.

La siguiente información de la aplicación se muestra en el panel de detalles de la Consola de la aplicación:

- Estado de Uso de Kaspersky Security Network.
- Estado de Protección del equipo.
- Información sobre las actualizaciones del módulo de aplicación y la base de datos.
- Datos de diagnóstico reales.
- Datos sobre las tareas de control del equipo.
- Información sobre la licencia.
- El estado de integración con Kaspersky Security Center: los detalles del equipo con Kaspersky Security Center instalado y al cual se conecta la aplicación; información sobre las tareas de la aplicación controlada por la directiva activa.

Se usan diferentes colores para indicar el estado de protección:

- *Verde*. La tarea se está ejecutando de acuerdo con los parámetros configurados. La protección está activa.
- *Amarillo*. La tarea no se inició, se pausó o se detuvo. Pueden ocurrir amenazas para la seguridad. Se le aconseja configurar e iniciar la tarea.
- *Rojo*. Se detectó una tarea completada con un error o una amenaza para la seguridad mientras la tarea se

ejecutaba. Se le aconseja iniciar la tarea o tomar medidas para eliminar la amenaza de la seguridad detectada.

Algunos detalles en este bloque (por ejemplo, los nombres de las tareas o el número de amenazas detectadas) son vínculos que, cuando se hace clic en ellos, abren el nodo de la tarea relevante o abren el registro de tareas.

La sección **Uso de Kaspersky Security Network** muestra el estado de la tarea actual, por ejemplo, *En ejecución*, *Detenida* o *Nunca ejecutada*. El indicador puede tener los siguientes valores:

- El color verde significa que la tarea Uso de KSN se está ejecutando y las solicitudes de estado de archivos se están enviando a KSN.
- El color amarillo significa que se acepta una de las declaraciones, pero la tarea no está en ejecución; o bien que la tarea está en ejecución, pero no se envían solicitudes de archivos a KSN.

Protección del equipo

La sección **Protección del equipo** (consulte la tabla a continuación) muestra información sobre el estado de protección actual del equipo.

Tabla 27. Información sobre el estado de protección del equipo

Sección Protección	Información
Indicador del estado de protección del equipo	El color del panel con el nombre de la sección refleja el estado de las tareas realizadas en dicha sección. El indicador puede tener los siguientes valores: • Verde – Este color se muestra de forma predeterminada y significa que el componente Protección de archivos en tiempo real está instalado y la tarea está en ejecución. • Amarillo – El componente Protección de archivos en tiempo real no está instalado, y la tarea Análisis de áreas críticas no se ha realizado hace mucho tiempo. • Rojo – La tarea Protección de archivos en tiempo real no está en ejecución.
Protección de archivos en tiempo real	**Estado de la tarea**: estado actual de la tarea, por ejemplo, *En ejecución* o *Detenida*. **Detectado**: número de objetos detectados por Kaspersky Embedded Systems Security. Por ejemplo, si Kaspersky Embedded Systems Security detecta un programa de malware en cinco archivos, el valor de este campo aumenta en uno. Si el número de programas de malware detectados supera 0, el valor se resalta en rojo.
Análisis de áreas críticas	**Fecha del último análisis**: fecha y hora del último análisis de áreas críticas en busca de virus y otras amenazas de seguridad informática. *Nunca ejecutado*: un evento que ocurre cuando la tarea de Análisis de áreas críticas no se ha realizado en los 30 días anteriores o más (valor predeterminado). Se puede cambiar el umbral para la generación de este evento.
Prevención de exploits	**Estado**: el estado actual de las técnicas de prevención de exploits, por ejemplo, *Aplicada* o *No aplicada*. **Modo de prevención**: uno de los dos modos disponibles, seleccionados durante configuración de protección de memoria de proceso: • Finalizar en caso de exploit. • Solo estadísticas. **Procesos protegidos**: el número total de procesos agregados al alcance de la protección y gestionados de acuerdo con el modo seleccionado.

Sección Protección	Información
Objetos con copia de seguridad	*Se superó el umbral de espacio disponible para Copia de seguridad*: este evento se produce cuando la cantidad de espacio libre en Copia de seguridad se está acercando al límite especificado. Kaspersky Embedded Systems Security continúa trasladando los objetos a Copia de seguridad. En este caso, el valor en el campo **Espacio usado** se resalta en amarillo. *Se superó el tamaño máximo de Copia de seguridad*: este evento se produce cuando el tamaño de Copia de seguridad ha alcanzado el límite especificado. Kaspersky Embedded Systems Security continúa trasladando los objetos a Copia de seguridad. En este caso, el valor en el campo **Espacio usado** se resalta en rojo. **Objetos con copia de seguridad**: cantidad de objetos que se encuentran actualmente en Copia de seguridad. **Espacio usado**: cantidad de espacio usado por la copia de seguridad.

Actualización

La sección **Actualización** (consulte la siguiente tabla) muestra información sobre cómo actualizar las bases de datos antivirus y los módulos de la aplicación.

Tabla 28. Información sobre el estado de los módulos y las bases de datos de Kaspersky Embedded Systems Security

Sección actualizaciones	Información
Indicador de estado de las bases de datos y los módulos del programa	El color del panel con el nombre de la sección refleja el estado de las bases de datos y los módulos de la aplicación. El indicador puede tener los siguientes valores: • Verde: este color se muestra de forma predeterminada, y significa que las bases de datos de la aplicación están actualizadas y que la última tarea de actualización de bases de datos se completó correctamente. • Amarillo: las bases de datos están desactualizadas o la última tarea de actualización de bases de datos produjo un error. • Rojo: se produjo el evento *Las bases de datos de la aplicación están obsoletas* o *Las bases de datos de la aplicación están dañadas*.

Sección actualizaciones	Información
Actualización de bases de datos y **Actualización de módulos del programa**	**Estado de las bases de datos**: un e valuación del estado de la actualización de bases de datos. Puede tener los valores siguientes: • **Las bases de datos de la aplicación están actualizadas**: las bases de datos de la aplicación se actualizaron hace no más de 7 días (predeterminado). • **Las bases de datos de la aplicación están desactualizadas**: las bases de datos de la aplicación se actualizaron hace 7 a 14 días (predeterminado). • **Las bases de datos de la aplicación son obsoletas**: las bases de datos de la aplicación se actualizaron hace más de 14 días (predeterminado). Se pueden cambiar los umbrales para la generación de los eventos *Las bases de datos de la aplicación están desactualizadas* y *Las bases de datos de la aplicación están obsoletas*. **Fecha de las bases de datos**: fecha y hora de publicación de la actualización de bases de datos más reciente. La fecha y la hora se especifican en formato UTC. **Estado de la última actualización de bases de datos**: fecha y hora de la última actualización de bases de datos. La fecha y hora se especifican de acuerdo con la hora local del equipo protegido. El campo aparece de color rojo si se produjo un evento con *Error*. **Actualizaciones de módulos disponibles**: número de actualizaciones del módulo de Kaspersky Embedded Systems Security disponibles para descargar e instalar. **Actualizaciones de módulos instaladas**: número de actualizaciones del módulo de Kaspersky Embedded Systems Security instaladas.

Control

La sección **Control** (consulte la tabla a continuación) muestra información sobre las tareas Control de inicio de aplicaciones, Control de dispositivos y Administración de firewall.

Tabla 29. Información sobre el estado de Control del equipo

Sección Control	Información
Indicador de estado de Control del equipo	El color del panel con el nombre de la sección refleja el estado de las tareas realizadas en dicha sección. El indicador puede tener los siguientes valores: • Verde: este color se muestra de forma predeterminada y significa que el componente Control de inicio de aplicaciones está instalado y la tarea se está ejecutando en el modo **Activo**. • Amarillo: Control de inicio de aplicaciones se está ejecutando en el modo **Solo estadísticas**. • Rojo: la tarea Control de inicio de aplicaciones no está en ejecución o ha generado errores.

Sección Control	Información
Control de inicio de aplicaciones	**Estado de la tarea**: estado actual de la tarea, por ejemplo, *En ejecución* o *Detenida*. **Modo**: uno de los dos modos disponibles para la tarea Control de inicio de aplicaciones: • Activo • Solo estadísticas **Inicios de aplicaciones denegados**: número de intentos de iniciar aplicaciones bloqueados por Kaspersky Embedded Systems Security durante la tarea de Control de inicio de aplicaciones. Si el número de inicios de aplicaciones bloqueados supera 0, el campo se muestra en rojo. **Tiempo promedio de procesamiento (ms)**: tiempo que le tomó a Kaspersky Embedded Systems Security procesar un intento de iniciar aplicaciones en el equipo protegido.
Control de dispositivos	**Estado de la tarea**: estado actual de la tarea, por ejemplo, *En ejecución* o *Detenida*. **Modo**: uno de dos modos disponibles de la tarea Control de dispositivos: • **Activo** • **Solo estadísticas** **Dispositivos bloqueados**: número de intentos de conexión de un dispositivo de almacenamiento masivo que fueron bloqueados por Kaspersky Embedded Systems Security durante la tarea de Control de dispositivos. Si el número de dispositivos de almacenamiento masivo bloqueados supera 0, el campo se muestra en rojo.
Administración de firewall	**Estado de la tarea**: estado actual de la tarea, por ejemplo, *En ejecución* o *Detenida*. **Intentos de conexiones bloqueados**: número de conexiones a un dispositivo protegido que fueron bloqueadas por las reglas especificadas en el firewall.

Diagnóstico

La sección **Diagnósticos** (consulte la tabla a continuación) muestra información sobre las tareas Inspección de registros y del Monitor de integridad de archivos.

Tabla 30. Información sobre estado de inspección del sistema

Sección Diagnóstico	Información
Indicador de estado del diagnóstico	El color del panel con el nombre de la sección refleja el estado de las tareas realizadas en dicha sección. El indicador puede tener los siguientes valores: • Verde: este color se muestra de forma predeterminada y significa que uno o los dos componentes de inspección del sistema están instalados y las tareas están en ejecución. • Amarillo: los dos componentes están instalados, pero una de las tareas de inspección del sistema no está en ejecución; se produjo el evento *No está en ejecución*. • Rojo: una de las tareas produjo un error.

Monitor de integridad de archivos	**Estado de la tarea**: estado actual de la tarea, por ejemplo, *En ejecución* o *Detenida*. **Operaciones de archivos no sancionadas**: número de cambios a archivos dentro del área de supervisión. Estos cambios pueden indicar que la seguridad de un equipo protegido ha sido violada.
Inspección de registros	**Estado de la tarea**: estado actual de la tarea, por ejemplo, *En ejecución* o *Detenida*. **Posibles transgresiones**: número de infracciones registradas según datos del registro de eventos de Windows. Este número se determina según las reglas de la tarea especificadas o el uso del analizador heurístico.

La información sobre la licencia de Kaspersky Embedded Systems Security se muestra en la fila ubicada en la esquina inferior izquierda del panel de detalles del nodo **Kaspersky Embedded Systems Security**.

Puede configurar las propiedades de Kaspersky Embedded Systems Security a través del vínculo Propiedades de la aplicación (consulte la sección “Configuración de Kaspersky Embedded Systems Security en la Consola de la aplicación” en la página 134).

Puede conectarse a otro equipo a través del siguiente vínculo **Conectarse a otro equipo** (consulte la sección “Administración de Kaspersky Embedded Systems Security mediante la Consola de la aplicación en otro equipo” en la página 146).

Interfaz de diagnóstico compacto

Esta sección describe cómo usar la Interfaz de diagnóstico compacto para revisar el estado del equipo o la actividad actual, y cómo configurar la escritura de archivos de volcado y de rastreo.

En este capítulo

Acerca de la Interfaz de diagnóstico compacto

El componente Interfaz de diagnóstico compacto (también denominado “CDI”) se instala y se desinstala junto con el componente Icono de la bandeja del sistema, de forma independiente respecto de la Consola de la aplicación, y puede usarse cuando la Consola de la aplicación no está instalada en el equipo protegido. CDI se inicia desde el Icono de la bandeja del sistema o ejecutando kavfsmui.exe desde la carpeta de la aplicación en el equipo.

Desde la ventana CDI, puede hacer lo siguiente:

- Revisar la información sobre el estado general de la aplicación (consulte la sección “Revisión del estado de Kaspersky Embedded Systems Security a través de la Interfaz de diagnóstico compacto” en la

página 164).

- Revisar los incidentes de seguridad que se han producido (consulte la sección “Revisión de estadísticas de eventos de seguridad”, en la página 165).
- Revisar la actividad actual en el equipo protegido (consulte la sección “Revisión de la actividad actual de la aplicación”, en la página 166).
- Iniciar o detener la escritura de los archivos de volcado y de rastreo (consulte la sección “Configuración de la escritura de los archivos de volcado y de rastreo”, en la página 167).
- Abra la Consola de la aplicación.
- Abra la ventana **Acerca de la aplicación** con la lista de actualizaciones instaladas y parches disponibles.

CDI está disponible incluso si el acceso a las funciones de Kaspersky Embedded Systems Security está protegido. No se requiere contraseña.

El componente CDI no puede configurarse mediante Kaspersky Security Center.

Revisión del estado de Kaspersky Embedded Systems Security a través de la Interfaz de diagnóstico compacto

► *Para abrir la ventana Interfaz de diagnóstico compacto, realice las siguientes acciones:*

1. Haga clic con el botón derecho en el icono de la bandeja del sistema de Kaspersky Embedded Systems Security, en el área de notificación de la barra de herramientas.
2. Seleccione la opción **Abrir Interfaz de diagnóstico compacto**.

   Se abre la ventana **Interfaz de diagnóstico compacto**.

Revise el estado actual de la clave, las tareas de protección del equipo en tiempo real y las tareas de actualización en la pestaña **Estado de protección**. Se utilizan diferentes colores para notificar al usuario sobre el estado de la protección (consulte la tabla a continuación).

Tabla 31. Estado de protección de la Interfaz de diagnóstico compacto.

Sección	Estado

Protección del equipo en tiempo real	El panel es *verde* para cualquiera de los siguientes escenarios (puede cumplirse cualquier cantidad de condiciones):
	• Configuración recomendada:
	  • Se inicia la tarea Protección de archivos en tiempo real con la configuración predeterminada.
	  • Se inicia la tarea Control de inicio de aplicaciones en modo **Activo** con la configuración predeterminada.
	• Configuración aceptable:
	  • El usuario configura la tarea Protección de archivos en tiempo real.
	  • Se modifica la configuración de la tarea de Control de inicio de aplicaciones.

Sección	Estado
	El panel es *amarillo* si se cumplen una o varias de las siguientes condiciones: • La tarea Protección de archivos en tiempo real está pausada (p el usuario o por la programación). • La tarea Control de inicio de aplicaciones se inicia en el modo **Solo estadísticas**. • Protección contra exploits y Control de inicio de aplicaciones se inician en el modo **Solo estadísticas**.
	El panel es *rojo* si se cumplen estas dos condiciones: • El componente Protección de archivos en tiempo real no está instalado, o la tarea está detenida o pausada. • El componente Control de inicio de aplicaciones no está instalado, o la tarea se inició en el modo **Solo estadísticas**.
Licencia	El panel es *verde* si la licencia actual es válida.
	Un panel *amarillo* significa que ha ocurrido uno de los siguientes eventos: • **Consultar el estado de la licencia**. • **La licencia caducará en 14 días y no se ha agregado ninguna clave adicional ni código de activación**. • **La clave agregada se ha colocado en una lista negra y se bloqueará**.
	Un panel *rojo* significa que ha ocurrido uno de los siguientes eventos: • **Aplicación no activada.** • **La licencia ha caducado.** • **Infracción del Contrato de licencia de usuario final.** • **La clave está en la lista negra.**
Actualización	El panel es *verde* cuando las bases de datos de la aplicación están actualizadas.
	El panel es *amarillo* cuando las bases de datos de la aplicación están desactualizadas.
	El panel es *rojo* cuando las bases de datos de la aplicación están obsoletas.

Revisión de estadísticas de eventos de seguridad

La pestaña **Estadísticas** muestra todos los eventos de seguridad. Cada estadística de la tarea de protección se muestra en un bloque independiente que especifica el número de incidentes, junto a la fecha y la hora en que ocurrió el último incidente. Cuando se registra un incidente, el color del bloque cambia a rojo.

► *Para revisar las estadísticas:*

1. Haga clic con el botón derecho en el icono de la bandeja del sistema de Kaspersky Embedded Systems Security, en el área de notificación de la barra de herramientas.
2. Seleccione la opción **Abrir Interfaz de diagnóstico compacto**.

   Se abre la ventana **Interfaz de diagnóstico compacto**.

3. Abra la pestaña **Estadísticas**.
4. Revise los incidentes de seguridad para las tareas de protección.

Revisión de la actividad de la aplicación actual

En esta pestaña, puede revisar el estado de las tareas y los procesos actuales de la aplicación, y obtener notificaciones rápidas sobre los eventos críticos que ocurren.

Los diferentes colores se usan para indicar el estado de la actividad de la aplicación:

- En la sección **Tareas**:
  - *Verde*. Ninguna condición para amarillo o rojo.
  - *Amarillo*. Las áreas críticas no se han analizado durante un periodo prolongado.
  - *Rojo*. Se cumple cualquiera de las siguientes condiciones:
    - No se inicia ninguna tarea, y no hay una programación de inicio configurada para ninguna de las tareas.
    - Los errores de inicio de aplicaciones se registran como eventos críticos.
- En la sección **Kaspersky Security Network**:
  - *Verde*. Se inicia la tarea Uso de KSN.
  - *Amarillo*. Se acepta la Declaración de KSN, pero no se inicia la tarea.

► *Para revisar la actividad de la aplicación actual en el equipo:*

1. Haga clic con el botón derecho en el icono de la bandeja del sistema de Kaspersky Embedded Systems Security, en el área de notificación de la barra de herramientas.
2. Seleccione la opción **Abrir Interfaz de diagnóstico compacto**.

   Se abre la ventana **Interfaz de diagnóstico compacto**.
3. Abra la pestaña **Actividad actual de la aplicación**.
4. Revise la siguiente información en la sección **Tareas**:
   - **Las áreas críticas no se han analizado durante un periodo prolongado**

     Este campo solo se muestra si la aplicación devuelve una advertencia correspondiente a un análisis de áreas críticas.
   - **En ejecución ahora**
   - **La ejecución produjo un error**
   - **Siguiente inicio definido por una programación**
5. Revise la siguiente información en la sección **Kaspersky Security Network**:
   - **KSN está activado. Los servicios de reputación de archivos están habilitados** o **La protección está desactivada**.
   - **estadísticas de la aplicación enviadas a KSN**.

La aplicación envía la información sobre malware, incluido el software fraudulento, detectado durante la tarea de Protección de archivos en tiempo real y las tareas de Análisis a pedido, así como la depuración de la información sobre errores durante el análisis.

El campo se muestra si se selecciona la casilla de verificación **Enviar estadísticas de Kaspersky Security Network** en la configuración de la tarea Uso de KSN.

6. Revise la siguiente información en la sección **Integración con Kaspersky Security Center**:
   - Se permite la administración local.
   - Se aplica la directiva: <Nombre del servidor de Kaspersky Security Center>.

Configuración de la escritura de archivos de rastreo y volcado

Puede configurar la escritura de archivos de rastreo y volcado mediante CDI.

También puede configurar el diagnóstico de mal funcionamiento a través de la Consola de la aplicación (consulte la sección “Configuración de Kaspersky Embedded Systems Security en la Consola de la aplicación” en la página 134).

► *Para empezar a escribir archivos de rastreo y de volcado, realice las siguientes acciones:*

1. Haga clic con el botón derecho en el icono de la bandeja del sistema de Kaspersky Embedded Systems Security, en el área de notificación de la barra de herramientas.
2. Seleccione la opción **Abrir Interfaz de diagnóstico compacto**.

   Se abre la ventana **Interfaz de diagnóstico compacto**.
3. Abra la pestaña **Solución de problemas**.
4. Cambie las siguientes opciones de rastreo, si es necesario:
   a. Seleccione la casilla de verificación **Escribir información de depuración para el archivo de rastreo en esta carpeta**.
   b. Haga clic en el botón **Examinar** para especificar la carpeta donde Kaspersky Embedded Systems Security guardará los archivos de rastreo.

      El rastreo se habilitará para todos los componentes con los parámetros predeterminados, utilizará el nivel de detalle establecido para la **Depuración** y el tamaño del registro máximo predeterminado de 50 MB.
5. Cambie las siguientes opciones del archivo de volcado, si es necesario:
   a. Seleccione la casilla de verificación **Crear archivo de volcado por mal funcionamiento en esta carpeta**.
   b. Haga clic en el botón **Examinar** para especificar la carpeta donde Kaspersky Embedded Systems Security guardará el archivo de volcado.
6. Haga clic en el botón **Aplicar**.

   Se aplicará una nueva configuración.

Actualización de los módulos del programa y las bases de datos de Kaspersky Embedded Systems Security

Esta sección brinda información sobre las tareas de actualización de las bases de datos y los módulos del programa de Kaspersky Embedded Systems Security, copias de actualizaciones y reversiones de actualizaciones de bases de datos de Kaspersky Embedded Systems Security, además de instrucciones sobre cómo configurar las tareas de actualización de las bases de datos y los módulos del programa.

En este capítulo

Acerca de las tareas de Actualización

Kaspersky Embedded Systems Security proporciona cuatro tareas de actualización del sistema: Actualización de bases de datos, Actualización de módulos del programa, Copia de actualizaciones y Reversión de la actualización de bases de datos.

De forma predeterminada, Kaspersky Embedded Systems Security se conecta con el origen de actualizaciones (uno de los equipos de actualizaciones de Kaspersky Lab) una vez por hora. Puede configurar todas las tareas de actualización (consulte la sección “Configuración de tareas de actualización”, en la página 174), excepto la tarea Reversión de la actualización de bases de datos. Cuando se modifica la configuración de una tarea, Kaspersky Embedded Systems Security aplicará los nuevos valores en el próximo inicio de la tarea.

No puede pausar y reanudar tareas de Actualización.

Actualización de bases de datos

De forma predeterminada, Kaspersky Embedded Systems Security copia las bases de datos del origen de actualizaciones al equipo protegido e inmediatamente comienza a usarlas ejecutando la tarea de Protección del equipo en tiempo real. Las tareas de Análisis a pedido empiezan a usar la base de datos actualizada en el siguiente inicio.

De forma predeterminada, Kaspersky Embedded Systems Security ejecuta la tarea de Actualización de bases de datos cada hora.

Actualización de módulos del programa

De forma predeterminada, Kaspersky Embedded Systems Security comprueba la disponibilidad de actualizaciones de módulos del programa en el origen de actualizaciones. Para empezar a utilizar los módulos del programa

instalados, se requiere un reinicio del equipo o un reinicio de Kaspersky Embedded Systems Security.

De forma predeterminada, Kaspersky Embedded Systems Security ejecuta la tarea de Actualización de módulos del programa cada semana los viernes a las 16:00 (hora según la configuración regional del equipo protegido). Durante la ejecución de la tarea, la aplicación examina la disponibilidad de las actualizaciones importantes y programadas de módulos de Kaspersky Embedded Systems Security sin distribuirlos.

Copia de actualizaciones

De forma predeterminada, durante la ejecución de la tarea, Kaspersky Embedded Systems Security descarga los archivos de la actualización de bases de datos y los guarda en la red especificada o en la carpeta local sin aplicarlos.

La tarea de Copia de actualizaciones está deshabilitada de forma predeterminada.

Reversión de la actualización de bases de datos

Durante la ejecución de la tarea, Kaspersky Embedded Systems Security vuelve a utilizar bases de datos con actualizaciones instaladas anteriormente.

La tarea de Reversión de la Actualización de bases de datos está deshabilitada de forma predeterminada.

Acerca de la actualización de módulos del programa de Kaspersky Embedded Systems Security

Kaspersky Lab puede emitir paquetes de actualización para los módulos de Kaspersky Embedded Systems Security. Los paquetes de actualización pueden ser *urgentes* (o *críticos*) y planificados. Los paquetes de actualización críticos reparan vulnerabilidades y errores; los paquetes planificados agregan nuevas funciones o mejoran las funciones existentes.

Los paquetes de actualización urgentes (críticos) se cargan en los servidores de actualizaciones de Kaspersky Lab. Su instalación automática puede configurarse usando la tarea de Actualización de módulos del programa. De forma predeterminada, Kaspersky Embedded Systems Security ejecuta la tarea de Actualización de módulos del programa cada semana los viernes a las 16:00 (hora según la configuración regional del equipo protegido).

Kaspersky Lab no publica paquetes de actualizaciones planificadas en los servidores de actualizaciones para la actualización automática; estos se deben descargar manualmente desde el sitio web de Kaspersky Lab. La tarea de Actualización de módulos del programa puede utilizarse para recibir información sobre la publicación de actualizaciones planificadas de Kaspersky Embedded Systems Security.

Las actualizaciones críticas se pueden descargar de Internet a cada equipo protegido o se puede utilizar un equipo como intermediario, copiando todas las actualizaciones en él y luego distribuyéndolas a los equipos de la red. Para copiar y guardar actualizaciones sin instalarlas, utilice la tarea de Copia de actualizaciones.

Antes de instalar las actualizaciones de los módulos, Kaspersky Embedded Systems Security crea copias de seguridad de los módulos instalados anteriormente. Si el proceso de actualización de los módulos del programa se interrumpe o genera un error, Kaspersky Embedded Systems Security volverá a usar automáticamente los módulos del programa instalados anteriormente. Los módulos del programa se pueden revertir manualmente a las actualizaciones anteriormente instaladas.

Durante la instalación de las actualizaciones descargadas, el servicio de Kaspersky Security se detiene y luego se inicia automáticamente.

Acerca de las actualizaciones de bases de datos de Kaspersky Embedded Systems Security

Las bases de datos de Kaspersky Embedded Systems Security almacenadas en el equipo protegido se desactualizan rápidamente. Los analistas de virus de Kaspersky Lab detectan cientos de nuevas amenazas diariamente, crean registros de identificación para ellas y las incluyen en las actualizaciones de las bases de datos de la aplicación. Las actualizaciones de las bases de datos son un archivo o un conjunto de archivos que contienen registros que identifican las amenazas descubiertas durante el tiempo desde que se creó la última actualización. Para mantener el nivel requerido de protección del equipo, se recomienda que las actualizaciones de las bases de datos se reciban en forma regular.

De forma predeterminada, si las bases de datos de Kaspersky Embedded Systems Security no se actualizan en un plazo de una semana a partir de la creación de las actualizaciones de las bases de datos instaladas, ocurre el evento *Las bases de datos de la aplicación están desactualizadas*. Si las bases de datos no se actualizan durante un periodo de dos semanas, ocurre el evento *La base de datos de la aplicación es obsoleta*. Aparece información sobre el estado de actualización de las bases de datos (consulte la sección “Visualización del estado de protección y de información sobre Kaspersky Embedded Systems Security” en la página 158) en el panel de detalles del nodo **Kaspersky Embedded Systems Security** del árbol de la consola de la aplicación. Puede usar la configuración general de Kaspersky Embedded Systems Security para indicar un número diferente de días antes de que estos eventos ocurran. También puede configurar las notificaciones del administrador sobre estos eventos (consulte la sección “Configuración de notificaciones de administradores y usuarios”, en la página 211).

Kaspersky Embedded Systems Security descarga las actualizaciones de las bases de datos y los módulos de la aplicación desde los servidores de actualizaciones FTP o HTTP de Kaspersky Lab, el servidor de administración de Kaspersky Security Center u otros orígenes de actualizaciones.

Las actualizaciones se pueden descargar en cada equipo protegido o se puede utilizar un equipo como intermediario para que copie todas las actualizaciones en él y luego las distribuya a los equipos. Si utiliza Kaspersky Security Center para la administración centralizada de la protección de los equipos de una organización, puede utilizar el servidor de administración de Kaspersky Security Center como intermediario para descargar las actualizaciones.

Las tareas de actualización de bases de datos pueden iniciarse manualmente o según una programación (consulte la sección "Configuración de las opciones de programación de inicio de tareas" en la página 149). De forma predeterminada, Kaspersky Embedded Systems Security ejecuta la tarea de Actualización de bases de datos cada hora.

Si el proceso de descarga de las actualizaciones se interrumpe o provoca un error, Kaspersky Embedded Systems Security volverá automáticamente a utilizar las bases de datos con las últimas actualizaciones instaladas. Si las bases de datos de Kaspersky Embedded Systems Security se dañan, se pueden revertir manualmente (consulte la sección “Reversión de las actualizaciones de la base de datos de Kaspersky Embedded Systems Security” en la página 180) a las actualizaciones anteriormente instaladas.

Esquemas para actualizar bases de datos y módulos de las aplicaciones antivirus que se usan en una organización

La selección del origen de actualizaciones en las tareas de actualización depende del esquema de actualización de las bases de datos y los módulos del programa que utiliza la organización.

Los módulos y bases de datos de Kaspersky Embedded Systems Security se pueden actualizar en los equipos protegidos mediante los esquemas siguientes:

- Descargar actualizaciones directamente de Internet a cada equipo protegido (Esquema 1)
- Descargar actualizaciones de Internet a un equipo intermediario y distribuirlas a equipos desde el equipo

  Cualquier equipo con los elementos de software enumerados a continuación instalados puede utilizarse como equipo intermediario:

  - Kaspersky Embedded Systems Security (Esquema 2).
  - Servidor de administración de Kaspersky Security Center (Esquema 3).

La actualización mediante un equipo intermediario no solo permitirá reducir el tráfico de Internet, sino también garantiza mayor seguridad para los equipos de la red.

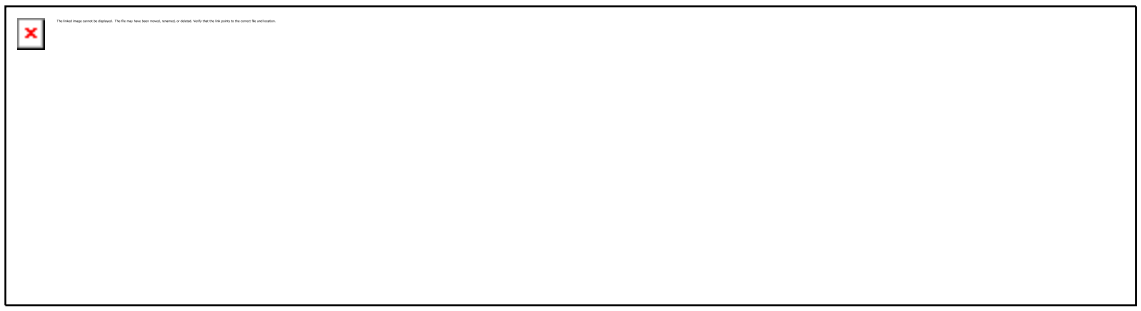
A continuación, se describen los esquemas de actualización enumerados.

Esquema 1. Actualización de bases de datos y módulos directamente desde Internet.

► *Para configurar actualizaciones de Kaspersky Embedded Systems Security directamente desde Internet:*

en cada equipo protegido, en la configuración de la tarea de Actualización de bases de datos y la tarea de Actualización de módulos del programa, especifique los servidores de actualizaciones de Kaspersky Lab como el origen de actualizaciones.

Se pueden configurar otros servidores HTTP o FTP que tengan una carpeta de actualización como la fuente de actualizaciones.

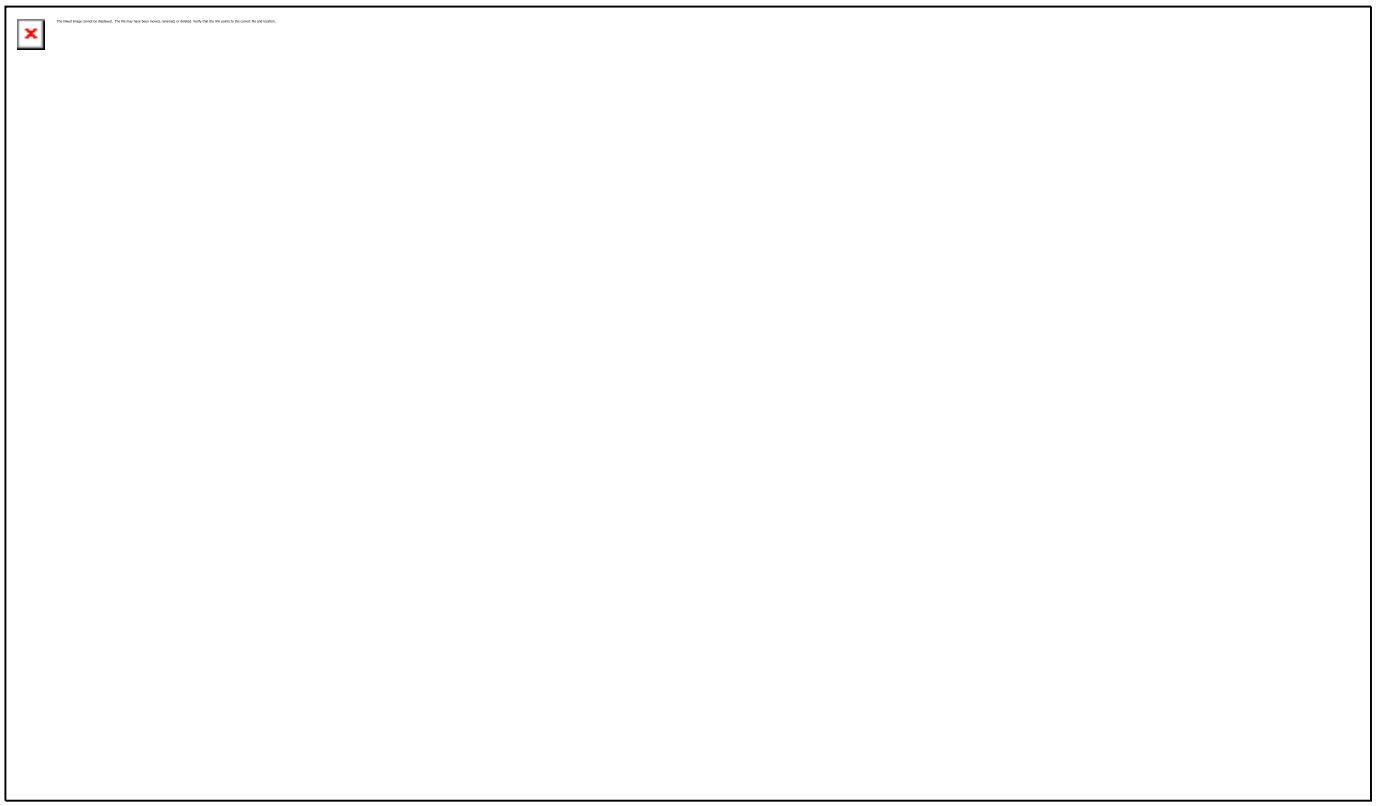


Esquema 2. Actualización de bases de datos y módulos a través de uno de los equipos protegidos.

► *Para configurar actualizaciones de Kaspersky Embedded Systems Security mediante uno de los equipos protegidos:*

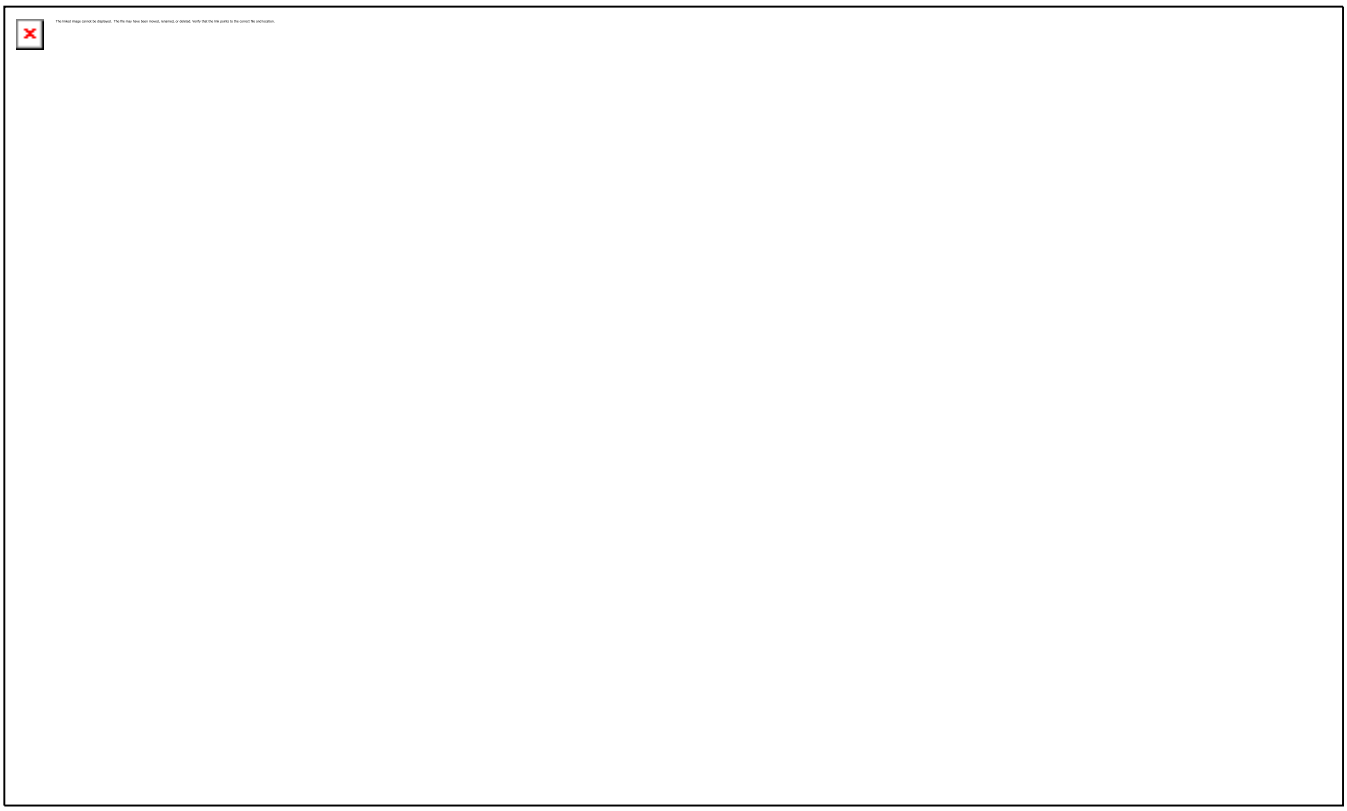
1. Copie las actualizaciones en el equipo protegido seleccionado. Para ello, realice las siguientes acciones:
   - Configure la tarea de Copia de actualizaciones en el equipo seleccionado:
     a. Especifique el servidor de actualizaciones de Kaspersky Lab como el origen de actualizaciones.
     b. Especifique una carpeta compartida para utilizar como la carpeta donde se guardan las actualizaciones.
2. Distribuya las actualizaciones a otros equipos protegidos. Para ello, realice las siguientes acciones:
   - En cada equipo protegido, configure la tarea de Actualización de bases de datos y de Actualización de módulos del programa (consulte la imagen a continuación).
     a. Como origen de actualizaciones, especifique la carpeta en la unidad del equipo intermediario en la cual se descargarán las actualizaciones.

Kaspersky Embedded Systems Security obtendrá actualizaciones mediante uno de los equipos protegidos.



Esquema 3. Actualización de bases de datos y módulos a través del Servidor de administración de Kaspersky Security Center

Si se utiliza la aplicación Kaspersky Security Center para la administración centralizada de la protección del equipo del antivirus, se pueden descargar las actualizaciones mediante el servidor de administración de Kaspersky Security Center instalado en la red de área local (consulte la figura a continuación).



► *Para configurar actualizaciones de Kaspersky Embedded Systems Security mediante el Servidor de administración de Kaspersky Security Center:*

1. Descargue las actualizaciones de los servidores de actualizaciones de Kaspersky Lab en el servidor de administración de Kaspersky Security Center. Para ello, realice las siguientes acciones:
   - Configure la tarea de Recuperar actualizaciones por el servidor de administración para el conjunto de equipos especificado:
     a. Especifique los servidores de actualizaciones de Kaspersky Lab como el origen de actualizaciones.
2. Distribuir actualizaciones a los equipos protegidos. Para esto, realice una de las siguientes acciones:
   - En Kaspersky Security Center, configure una tarea de grupo de Actualización de bases de datos (módulo de aplicación) del antivirus para distribuir las actualizaciones en los equipos protegidos:
     a. En la programación de la tarea, especifique **Después de que el Servidor de administración obtenga las actualizaciones** como la frecuencia de inicio.

        El servidor de administración iniciará la tarea cada vez que reciba actualizaciones (método recomendado).

        La frecuencia de inicio **Después de que el servidor de administración obtenga las actualizaciones** no se puede especificar en la Consola de la aplicación.

- En cada equipo protegido, configure la tarea de Actualización de bases de datos y de Actualización de módulos del programa:
  a. Especifique el servidor de administración de Kaspersky Security Center como origen de actualizaciones.
  b. Configure la programación de la tarea de ser necesario.

  > Si la base de datos antivirus de Kaspersky Embedded Systems Security se actualiza con poca frecuencia (entre una vez al mes y una vez al año), la probabilidad de descubrir amenazas se reducirá y la frecuencia de falsas alarmas que surjan debido a los componentes de la aplicación aumentará.

  Kaspersky Embedded Systems Security obtendrá actualizaciones mediante el Servidor de administración de Kaspersky Security Center.

Si planea utilizar el Servidor de administración de Kaspersky Security Center para distribuir las actualizaciones, instale el Agente de red, un componente de aplicación incluido en el kit de distribución de Kaspersky Security Center, en cada uno de los equipos protegidos. Esto garantiza la interacción entre el Servidor de administración y Kaspersky Embedded Systems Security en el equipo protegido. Se proporciona información detallada sobre el Agente de red y su configuración con Kaspersky Security Center en la *Ayuda de Kaspersky Security Center.*

Configuración de tareas de actualización

Esta sección proporciona instrucciones sobre cómo configurar tareas de Actualización de Kaspersky Embedded Systems Security.

En esta sección

Configuración de las opciones para trabajar con orígenes de actualizaciones de Kaspersky Embedded Systems Security

Para cada tarea de actualización excepto la tarea de Reversión de la actualización de bases de datos, puede especificar uno o varios orígenes de actualizaciones, agregar orígenes de actualizaciones definidas por los usuarios y configurar la conexión con las fuentes especificadas.

> Después de que la configuración de la tarea de actualización se modifica, la nueva configuración no se aplicará inmediatamente en las tareas de actualización en ejecución. La configuración solo se aplicará cuando la tarea se reinicie.

► *Para especificar el tipo de origen de actualizaciones:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
2. Seleccione el nodo secundario correspondiente a la tarea de actualización que desea configurar.
3. Haga clic en el vínculo **Propiedades** en el panel de detalles del nodo seleccionado.

   Se abre la ventana **Configuración de tareas** en la pestaña **General**.
4. En la sección **Origen de actualizaciones**, seleccione el tipo de origen de actualizaciones de Kaspersky Embedded Systems Security:
   - **Servidor de administración de Kaspersky Security Center**

     Kaspersky Embedded Systems Security usa el Servidor de Administración de Kaspersky Security Center como origen de actualizaciones.

     Solo puede seleccionar esta opción si las aplicaciones de Kaspersky Lab en su red se administran con el sistema de acceso remoto de Kaspersky Security Center y si el Agente de red (el componente de Kaspersky Security Center que proporciona la conexión entre los equipos y el Servidor de administración) está instalado en el equipo protegido.
   - **Servidores de actualizaciones de Kaspersky Lab**

     Kaspersky Embedded Systems Security usa sitios web de Kaspersky Lab como orígenes de actualizaciones, ya que alojan actualizaciones para las bases de datos y los módulos de programas de todos los productos de la empresa.

     De forma predeterminada, esta opción está seleccionada.
   - **Servidores FTP o HTTP personalizados o carpetas de red**

     Kaspersky Embedded Systems Security usa el servidor HTTP o FTP especificado por el administrador o carpetas en equipos de red locales como origen de actualizaciones.

     Se puede crear una lista de fuentes con las actualizaciones actuales haciendo clic en el vínculo **Servidores FTP o HTTP personalizados o carpetas de red**.
5. Si es necesario, establezca la configuración avanzada para los orígenes de actualizaciones definidas por los usuarios:
   a. Haga clic en el vínculo **Servidores FTP o HTTP personalizados o carpetas de red**.
      i. En la ventana **Servidores de actualizaciones** que se abre, seleccione o desactive las casillas de verificación al lado de los orígenes de actualizaciones definidas por los usuarios para iniciar o finalizar su uso.
      ii. Haga clic en **Aceptar**.
   b. En la sección **Origen de actualizaciones**, en la pestaña **General**, seleccione o desactive la casilla **Usar los servidores de actualizaciones de Kaspersky Lab si no están disponibles los servidores especificados**.

      Esta casilla de verificación habilita o deshabilita la opción de usar servidores de actualizaciones de Kaspersky Lab como origen de actualizaciones si los orígenes de actualizaciones definidos por los usuarios no están disponibles.

      Si se activa la casilla, se habilita esta función.

      De forma predeterminada, la casilla está activada.

      Se puede activar la casilla **Usar los servidores de actualizaciones de Kaspersky Lab**

si no están disponibles los servidores especificados cuando se habilita la opción **Servidores FTP o HTTP personalizados o carpetas de red**.

6. En la ventana **Configuración de tareas**, seleccione la pestaña **Configuración de conexión** para establecer la configuración y conectarse con los orígenes de actualizaciones:

   - Desactive o seleccione la casilla de verificación **Usar servidor proxy para los servidores de actualizaciones de Kaspersky Lab**.

     La casilla habilita/deshabilita el uso de la configuración del servidor proxy si se reciben actualizaciones desde los servidores de Kaspersky Lab o si la casilla **Usar los servidores de actualizaciones de Kaspersky Lab si no están disponibles los servidores especificados** está seleccionada.

     Si se activa la casilla, se usa la configuración del servidor proxy.

     Si se desactiva la casilla, no se usa la configuración del servidor proxy.

     De forma predeterminada, la casilla está activada.

   - Desactive o seleccione la casilla de verificación **Usar servidor proxy para otros servidores**.

     La casilla de verificación habilita o deshabilita el uso de la configuración del servidor proxy si **Servidores FTP o HTTP personalizados o carpetas de red** está seleccionado como origen de actualizaciones.

     Si se activa la casilla, se usa la configuración del servidor proxy.

     De forma predeterminada, la casilla está desactivada.

   Para obtener información sobre cómo establecer la configuración del servidor proxy opcional y la configuración de autenticación para acceder al servidor proxy, consulte la sección Inicio y configuración de la tarea de Actualización de bases de datos de Kaspersky Embedded Systems Security.

7. Haga clic en **Aceptar**.

La configuración establecida para el origen de actualizaciones de Kaspersky Embedded Systems Security se guardará y se aplicará en el siguiente inicio de la tarea.

Puede administrar la lista de orígenes de actualizaciones definidas por los usuarios de Kaspersky Embedded Systems Security.

► *Para modificar la lista de orígenes de actualizaciones de aplicación definidas por los usuarios:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
2. Seleccione el nodo secundario correspondiente a la tarea de actualización que desea configurar.
3. Haga clic en el vínculo **Propiedades** en el panel de detalles del nodo seleccionado.

   Se abre la ventana **Configuración de tareas** en la pestaña **General**.
4. Haga clic en el vínculo **Servidores FTP o HTTP personalizados o carpetas de red**.

   Se abre la ventana **Servidores de actualizaciones**.
5. Haga lo siguiente:

   - Para agregar un origen de actualizaciones definido por el usuario, en el campo de entrada, defina la dirección de la carpeta que contiene los archivos de actualización en el servidor FTP o HTTP, y especifique una carpeta local o de red en formato UNC (convención de nomenclatura universal).

Presione **ENTER**.

De forma predeterminada, la carpeta agregada se utiliza como origen de actualizaciones.

- Para deshabilitar el uso de un origen definido por el usuario, desactive la casilla de verificación al lado del origen en la lista.
- Para habilitar el uso de un origen definido por el usuario, seleccione la casilla de verificación al lado del origen en la lista.
- Para cambiar el orden en el que Kaspersky Embedded Systems Security accede a los orígenes de actualizaciones definidos por el usuario, utilice los botones **Subir** y **Bajar** para mover el origen seleccionado al comienzo o al final de la lista, según si se debe usar antes o después de otras fuentes.
- Para cambiar la ruta del origen, seleccione el origen en la lista y haga clic en el botón **Editar**, realice los cambios necesarios en el campo de entrada y presione la tecla **INTRO**.
- Para eliminar un origen definido por el usuario, selecciónelo en la lista y presione el botón **Eliminar**.

> No es posible eliminar el único origen definido por el usuario restante de la lista.

6. Haga clic en **Aceptar**.

Se guardarán los cambios en la lista de orígenes de actualizaciones de la aplicación definidas por los usuarios.

Optimización del uso de la lectura y escritura en disco al ejecutar la tarea de Actualización de bases de datos

Al ejecutar la tarea de Actualización de bases de datos, Kaspersky Embedded Systems Security almacena archivos de actualización en el disco local del equipo. Puede reducir la carga de trabajo en el subsistema de lectura y escritura en disco del equipo mediante el almacenamiento de archivos de actualización en una unidad virtual en la RAM al ejecutar la tarea de actualización.

> Esta función está disponible para los sistemas operativos Microsoft Windows 7 y superiores.

> Cuando se usa esta función mientras se ejecuta la tarea Actualización de bases de datos, es posible que aparezca una unidad lógica adicional en el sistema. Esta unidad lógica se eliminará del sistema operativo después de que la tarea se complete.

► *Para reducir la carga de trabajo en el subsistema de lectura y escritura en disco de su equipo durante la tarea Actualización de bases de datos, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
2. Seleccione el nodo secundario **Actualización de bases de datos**.
3. Haga clic en el vínculo **Propiedades** en el panel de detalles del nodo **Actualización de bases de datos**.
4. Se abre la ventana **Configuración de tareas** en la pestaña **General**.
5. En la sección Optimización de lectura y escritura en disco, defina la siguiente configuración:
   - Desactive o seleccione la casilla de verificación **Reducir la carga de lectura y escritura en disco**.

     Esta casilla de verificación habilita o deshabilita la función de optimización del

subsistema del disco mediante el almacenamiento de archivos de actualización en una unidad virtual en la RAM.

Si se activa la casilla, se habilita esta función.

De forma predeterminada, la casilla está desactivada.

- En el campo **RAM usada para la optimización, MB**, especifique el volumen de RAM (en MB). El sistema operativo asigna temporalmente el volumen de RAM especificado para almacenar archivos de actualización al ejecutar la tarea. El tamaño de RAM predeterminado es 512 MB. El tamaño de RAM mínimo es 400 MB.

6. Haga clic en **Aceptar**.

Las opciones configuradas se guardarán y se aplicarán en el siguiente inicio de la tarea.

Configuración de parámetros de la tarea Copia de actualizaciones

► *Para configurar la tarea Copia de actualizaciones:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
2. Seleccione el nodo secundario **Copia de actualizaciones**.
3. Haga clic en el vínculo **Propiedades** en el panel de detalles del nodo **Copia de actualizaciones**.

   Se abre la ventana **Configuración de tareas**.
4. En las pestañas **General** y **Configuración de conexión**, configure las opciones para trabajar con fuentes de actualizaciones (consulte la sección “Configuración de las opciones para trabajar con fuentes de actualizaciones de Kaspersky Embedded Systems Security” en la página 174).
5. En la pestaña **General** en la sección **Configuración de la copia de actualizaciones**:
   - Especifique las condiciones para la copia de actualizaciones:
     - **Copiar actualizaciones de las bases de datos**.

       Kaspersky Embedded Systems Security solo descarga actualizaciones de las bases de datos del software.

       De forma predeterminada, esta opción está seleccionada.
     - **Copiar actualizaciones críticas de módulos del programa**.

       Kaspersky Embedded Systems Security solo descarga actualizaciones urgentes de módulos del programa de Kaspersky Embedded Systems Security.
     - **Copiar actualizaciones de bases de datos y actualizaciones críticas de módulos del programa**.

       Kaspersky Embedded Systems Security descarga actualizaciones de las bases de datos del programa y actualizaciones críticas de módulos del programa de Kaspersky Embedded Systems Security.
   - Especifique la carpeta local o de red a la cual Kaspersky Embedded Systems Security distribuirá las actualizaciones descargadas.

6. En las pestañas **Programación** y **Avanzado**, configure la programación de inicio de tareas (consulte la sección “Configuración de las opciones de programación de inicio de tareas", en la página 149).
7. En la pestaña **Ejecutar como**, configure la tarea que se iniciará con permisos de la cuenta (consulte la sección “Especificación de una cuenta de usuario para iniciar una tarea”, en la página 151).
8. Haga clic en **Aceptar**.

Las opciones configuradas se guardarán y se aplicarán en el siguiente inicio de la tarea.

Configuración de tareas de Actualización de módulos del programa

► *Para configurar la tarea de Actualización de módulos del programa:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
2. Seleccione el nodo secundario **Actualización de módulos del programa**.
3. Haga clic en el vínculo **Propiedades** en el panel de detalles del nodo **Actualización de módulos del programa**.

   Se abre la ventana **Configuración de tareas**.
4. En las pestañas **General** y **Configuración de conexión**, configure las opciones para trabajar con fuentes de actualizaciones (consulte la sección “Configuración de las opciones para trabajar con fuentes de actualizaciones de Kaspersky Embedded Systems Security” en la página 174).
5. En la pestaña **General** de la sección **Configuración de actualización de la aplicación**, configure las opciones para actualizar módulos de la aplicación:

   - **Buscar solo actualizaciones críticas del programa**

     Kaspersky Embedded Systems Security muestra una notificación sobre las actualizaciones urgentes de módulos del programa disponibles en el origen de actualizaciones sin descargar las actualizaciones. La notificación se muestra si las notificaciones sobre los eventos de este tipo se han habilitado.

     De forma predeterminada, esta opción está seleccionada.

   - **Copiar e instalar actualizaciones críticas de módulos del programa**

     Kaspersky Embedded Systems Security descarga e instala actualizaciones críticas a módulos del programa.

   - **Permitir el reinicio del sistema operativo**

     El sistema operativo se reinicia después de instalar actualizaciones que requieren un reinicio.

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security reinicia el sistema operativo después de instalar actualizaciones que requieren un reinicio.

     Esta casilla de verificación está activa si la opción **Copiar e instalar actualizaciones críticas de módulos del programa** está seleccionada.

     De forma predeterminada, la casilla está desactivada.

   - **Informarme de las actualizaciones programadas que estén disponibles para los módulos del programa**

     Las notificaciones sobre todas las actualizaciones programadas de los módulos del programa de Kaspersky Embedded Systems Security disponibles en el origen de

actualizaciones se muestran. La aplicación muestra una notificación si las notificaciones están habilitadas para eventos de este tipo.

Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security muestra una notificación sobre todas las actualizaciones programadas de los módulos del programa disponibles en el origen de actualizaciones.

De forma predeterminada, la casilla está activada.

6. En las pestañas **Programación** y **Avanzado**, configure la programación de inicio de tareas (consulte la sección “Configuración de las opciones de programación de inicio de tareas", en la página 149). De forma predeterminada, Kaspersky Embedded Systems Security ejecuta la tarea de Actualización de módulos del programa cada semana los viernes a las 16:00 (hora según la configuración regional del equipo protegido).
7. En la pestaña **Ejecutar como**, configure la tarea que se iniciará con permisos de la cuenta (consulte la sección “Especificación de una cuenta de usuario para iniciar una tarea", en la página 151).
8. Haga clic en **Aceptar**.

Las opciones configuradas se guardarán y se aplicarán en el siguiente inicio de la tarea.

Kaspersky Lab no publica paquetes de actualizaciones planificadas en los servidores de actualizaciones para la instalación automática; se deben descargar manualmente desde el sitio web de Kaspersky Lab. Se puede configurar una notificación para el administrador sobre el evento *Está disponible una nueva actualización programada de módulos del programa*; dicha notificación contendrá la dirección URL de la página del sitio web desde la que se pueden descargar las actualizaciones programadas.

Reversión de actualizaciones de bases de datos de Kaspersky Embedded Systems Security

Antes de que se apliquen las actualizaciones de las bases de datos, Kaspersky Embedded Systems Security crea copias de seguridad de las bases de datos anteriormente usadas. Si la actualización se interrumpió o arrojó un error, Kaspersky Embedded Systems Security volverá automáticamente a usar las bases de datos anteriormente instaladas.

Si se produce algún problema después de la actualización de bases de datos, es posible revertir a las actualizaciones instaladas anteriormente mediante la tarea Reversión de la actualización de bases de datos.

► *Para iniciar la tarea Reversión de la actualización de bases de datos:*

Haga clic en el vínculo **Iniciar** en el panel de detalles del nodo **Reversión de la actualización de bases de datos**.

Reversión de actualizaciones del módulo de aplicación

Los nombres de configuración pueden variar en los diferentes sistemas operativos Windows.

Antes de aplicar actualizaciones de módulos del programa, Kaspersky Embedded Systems Security crea copias de seguridad de los módulos actualmente en uso. Si el proceso de actualización de los módulos se interrumpió o arrojó un error, Kaspersky Embedded Systems Security volverá automáticamente a usar los módulos con las

últimas actualizaciones instaladas.

Para revertir los módulos del programa, utilice el componente de Microsoft Windows para **instalar y eliminar aplicaciones**.

Estadísticas de las tareas de actualización

Durante la ejecución de la tarea de actualización, es posible visualizar información en tiempo real sobre la cantidad de datos descargados desde que se inició la tarea hasta el momento actual, además de otras estadísticas de ejecución de la tarea.

Cuando la tarea finaliza o se detiene, puede ver esta información en el registro de tareas.

► *Para ver las estadísticas de las tareas de actualización, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
2. Seleccione el nodo secundario que corresponda a la tarea cuyas estadísticas desea ver.

   Las estadísticas de la tarea se muestran en la sección **Estadísticas** del panel de detalles del nodo seleccionado.

Si está viendo la tarea de Actualización de bases de datos o la tarea de Copia de actualizaciones, el bloque **Estadísticas** muestra el volumen de datos descargados por Kaspersky Embedded Systems Security en el momento actual (**Datos recibidos**).

Si está visualizando la tarea de Actualización de módulos del programa, verá la información descrita en la siguiente tabla.

Tabla 32. Información sobre la tarea de Actualización de módulos del programa

Campo	Descripción
Datos recibidos	Cantidad total de datos descargados.
Actualizaciones críticas disponibles	Cantidad de actualizaciones críticas disponibles para instalar.
Actualizaciones programadas disponibles	Cantidad de actualizaciones planificadas disponibles para la instalación.
Errores al aplicar las actualizaciones	Si el valor de este campo no es cero, la actualización no se aplicó. Se puede ver el nombre de la actualización que causó un error durante su aplicación en el registro de tareas (consulte la sección “Ver información y estadísticas de una tarea de Kaspersky Embedded Systems Security en los registros” en la página 202).

Aislamiento de objetos y creación de copias de seguridad

Esta sección proporciona información sobre las copias de seguridad de los objetos maliciosos detectados antes de su desinfección o eliminación, y sobre poner en cuarentena a los objetos probablemente infectados.

En este capítulo

Cómo aislar objetos probablemente infectados. Cuarentena

En esta sección se describe cómo aislar objetos probablemente infectados poniéndolos en cuarentena y cómo configurar las opciones de Cuarentena.

En esta sección

Acerca de la puesta en cuarentena de objetos probablemente infectados

Kaspersky Embedded Systems Security pone en cuarentena los objetos probablemente infectados al pasarlos de su ubicación original a la carpeta de *Cuarentena*. Por razones de seguridad, los objetos son puestos en la carpeta de Cuarentena en forma cifrada.

Visualización de objetos en cuarentena

Los objetos en cuarentena se pueden visualizar en el nodo **Cuarentena** de la consola de la aplicación.

► *Para ver los objetos en cuarentena, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Cuarentena**.

La información sobre los objetos en cuarentena se muestra en el panel de detalles del nodo seleccionado.

► *Para encontrar el objeto requerido en la lista de Objetos en cuarentena,*

ordene los objetos (consulte la sección “Cómo ordenar los objetos en Cuarentena”, en la página 183) o filtre los objetos (consulte la sección “Filtrado de los objetos en Cuarentena”, en la página 183).

En esta sección

Cómo ordenar los objetos en Cuarentena

De manera predeterminada, los objetos en la lista de objetos en cuarentena se ordenan por la fecha de ingreso en cuarentena en orden cronológico inverso. Para buscar el objeto deseado, puede ordenar los objetos por columnas con información sobre los objetos. El resultado de la clasificación se guardará si cierra y vuelve a abrir el nodo **Cuarentena**, o si cierra la Consola de la aplicación, guarda el archivo msc y vuelve a abrirla desde este archivo.

► *Para ordenar objetos, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Cuarentena**.
3. En el panel de detalles del nodo **Cuarentena**, seleccione el encabezado de columna que desea usar para ordenar los objetos en la lista.

Los objetos en la lista se ordenarán según el parámetro seleccionado.

Filtrado de objetos en cuarentena

Para buscar el objeto en cuarentena requerido, puede filtrar los objetos de la lista: mostrar sólo los objetos que satisfagan los criterios de filtrado (filtros) que especifique. Los resultados filtrados se guardarán si cierra y vuelve a abrir el nodo **Cuarentena** o si cierra la consola de la aplicación, guarda el archivo msc y vuelve a abrirlo desde este archivo.

► *Para especificar uno o varios filtros, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Cuarentena**.
3. Seleccione **Filtrar** en el menú contextual del nombre del nodo.

   Se abre la ventana **Configuración de filtro**.
4. Para agregar un filtro, siga estos pasos:
   a. En el **Nombre del campo**, seleccione un elemento con el que desea comparar el valor de filtro.
   b. En la lista **Operador**, seleccione la condición de filtrado. Los valores de las condiciones de filtrado en la lista pueden diferir según el valor que haya seleccionado en la lista **Nombre del campo**.
   c. Introduzca el valor de filtro en el campo **Valor del campo** o selecciónelo de la lista.
   d. Haga clic en el botón **Agregar**.

   El filtro que agregó aparecerá en la lista de filtros en la ventana **Configuración de filtro**. Repita los pasos

A a D para cada filtro que agregue. Use las siguientes directrices mientras trabaja con los filtros:

- Para combinar varios filtros mediante el operador lógico "AND", seleccione **Si se cumplen todas las condiciones**.
- Para combinar varios filtros mediante el operador lógico "OR", seleccione **Si se cumple alguna condición**.
- Para eliminar un filtro, seleccione el filtro que desea eliminar en la lista de filtros y haga clic en el botón **Eliminar**.
- Para editar un filtro, seleccione el filtro de la lista en la ventana **Configuración de filtro**. Luego, cambie los valores requeridos en el campo **Nombre del campo**, **Operador** o **Valor del campo** y haga clic en el botón **Reemplazar**.

5. Después de haber agregado todos los filtros, haga clic en el botón **Aplicar**.

Se guardarán los filtros creados.

► *Para volver a mostrar todos los objetos de la lista de objetos en cuarentena,*

seleccione **Eliminar** el filtro en el menú contextual del nodo **Cuarentena**.

Análisis de archivos en cuarentena

De forma predeterminada, después de cada actualización de bases de datos, Kaspersky Embedded Systems Security realiza la tarea del sistema de Análisis de archivos en cuarentena. La configuración de la tarea se describe en la tabla a continuación. La configuración de la tarea de Análisis de archivos en cuarentena no se puede modificar.

Puede configurar la programación de inicio de tareas (consulte la sección “Configuración de la programación de inicio de tareas” en la página 149), iníciela manualmente y modifique los permisos de la cuenta (consulte la sección “Especificación de una cuenta de usuario para iniciar una tarea” en la página 151) utilizados para iniciar la tarea.

Una vez analizados los objetos en cuarentena después de actualizar sus bases de datos, es posible que Kaspersky Embedded Systems Security vuelva a clasificar algunos objetos como no infectados: el estado de dichos objetos cambiará a **Falsa alarma**. Otros objetos pueden clasificarse como infectados, en cuyo caso Kaspersky Embedded Systems Security gestiona tales objetos según lo especificado por la configuración de la tarea de Análisis de archivos en cuarentena: desinfectar, o eliminar si la desinfección produjera un error.

Tabla 33. Configuración de la tarea de Análisis de archivos en cuarentena

Configuración de la tarea de Análisis de archivos en cuarentena	Valor
Área del análisis	Carpeta de cuarentena
Configuración de seguridad	Común para toda el área del análisis. Los valores se proporcionan en la tabla a continuación.

Tabla 34. Configuración del análisis en la tarea de Análisis de archivos en cuarentena

Configuración de seguridad	Valor
Analizar objetos	Todos los objetos incluidos en el área del análisis
Optimización	Deshabilitado

Configuración de seguridad	Valor
Acción para realizar con los objetos infectados y otros detectados	Desinfectar. Si la desinfección es imposible, eliminar
Acción para realizar en los objetos infectados	Omitir
Excluir objetos	No
No detectar	No
Detener el análisis si demora más de (seg)	No configurado
Omitir objetos de más de (MB)	No configurado
Analizar secuencias alternativas de NTFS	Habilitado
Sectores de inicio de unidades y MBR	Deshabilitado
Uso de la tecnología iChecker	Deshabilitado
Uso de la tecnología iSwift	Deshabilitado
Analizar objetos compuestos	• Archivos* • Archivos SFX* • Objetos empaquetados* • Objetos OLE integrados* * La opción Analizar solo los archivos nuevos y modificados está deshabilitada.
Buscar firmas de Microsoft en archivos	No se realizó
Usar el analizador heurístico	Habilitado con nivel de análisis **Profundo**
Zona de confianza	No aplicado

Restauración de objetos en cuarentena

Kaspersky Embedded Systems Security coloca los objetos probablemente infectados en la carpeta de cuarentena en forma cifrada para proteger al equipo contra sus posibles efectos perjudiciales.

Puede restaurar cualquier objeto de la cuarentena. Esto puede resultar necesario en los siguientes casos:

- Si después del análisis de archivos en cuarentena mediante el uso de las bases de datos actualizadas, el estado de un objeto cambió a **Falsa alarma** o **Desinfectados**.
- Si considera que el objeto no es peligroso para el equipo y desea utilizarlo. Si no desea que Kaspersky Embedded Systems Security aísle este objeto durante los análisis sucesivos, puede excluir el objeto del procesamiento en la tarea de Protección de archivos en tiempo real y en las tareas de Análisis a pedido. Para ello, especifique el objeto con el valor de configuración de seguridad **Excluir archivos** (por nombre de archivo) o **No detectar** en esas tareas, o bien agréguelo a la Zona de confianza (en la página 441).

Al restaurar objetos, puede seleccionar la ubicación de almacenamiento para el objeto restaurado: ubicación original (de manera predeterminada), carpeta especial para objetos restaurados en el equipo protegido o carpeta personalizada en el equipo en que está instalada la Consola de la aplicación, o bien en otro equipo de la red.

La opción **Restaurar a carpeta** se utiliza para almacenar objetos restaurados en el equipo protegido. Puede configurar los valores de seguridad especiales para que se realice su análisis. La ruta a esta carpeta está definida por la configuración de Cuarentena.

Restaurar objetos de la cuarentena puede hacer que el equipo se infecte.

Puede restaurar el objeto y guardar su copia en la carpeta de cuarentena para su uso posterior, por ejemplo, a fin de volver a analizar el objeto después de que se haya actualizado la base de datos.

Si un objeto en cuarentena estaba incluido en un objeto compuesto (por ejemplo, en un archivo), Kaspersky Embedded Systems Security no lo incluirá en el objeto compuesto durante la restauración; en su lugar, lo guardará de forma separada en una carpeta seleccionada.

Puede restaurar uno o varios objetos.

► *Para restaurar objetos en cuarentena, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Cuarentena**.
3. En el panel de detalles del nodo **Cuarentena**, realice una de las siguientes acciones:
   - Para restaurar un objeto, seleccione **Restaurar** desde el menú contextual del objeto que desea restaurar.
   - Para restaurar varios objetos, seleccione los objetos que desea restaurar mediante la tecla **CTRL** o **MAYÚS**, haga clic con el botón secundario en uno de los objetos seleccionados y seleccione **Restaurar** en el menú contextual.

   Se abre la ventana **Restaurar objeto**.
4. En la ventana **Restaurar objeto**, especifique la carpeta donde se guardará el objeto que se está restaurando para cada objeto seleccionado.

   El nombre del objeto restaurado se muestra en el campo **Objeto** en la parte superior de la ventana. Si selecciona varios objetos, se mostrará el nombre del primer objeto en la lista de objetos seleccionados.
5. Realice uno de los siguientes pasos:
   - Para restaurar un objeto a su ubicación original, seleccione **Restaurar a la carpeta de origen**.
   - Para restaurar un objeto a la carpeta especificada como la ubicación para los objetos restaurados en la configuración, seleccione **Restaurar a la carpeta de restauración predeterminada**.
   - Para guardar un objeto en una carpeta diferente en el equipo en que está instalada la Consola de la aplicación o en una carpeta compartida, seleccione **Restaurar a una carpeta del equipo local o de un recurso de red** y, a continuación, seleccione la carpeta necesaria o especifique una ruta a esta.
6. Si desea guardar una copia del objeto en la carpeta de Cuarentena después de que se lo haya restaurado, desactive la casilla de verificación **Eliminar objetos del depósito una vez restaurados**.
7. Para aplicar las condiciones de restauración especificadas en los restantes objetos seleccionados, active la casilla de verificación **Aplicar a todos los objetos seleccionados**.

   Todos los objetos seleccionados se restaurarán y se guardarán en la ubicación especificada: si seleccionó **Restaurar a la carpeta de origen**, cada uno de los objetos se guardará en su ubicación original; si seleccionó **Restaurar a la carpeta de restauración predeterminada** o **Restaurar a una carpeta del equipo local o de un recurso de red**, todos los objetos se guardarán en la carpeta especificada.

8. Haga clic en **Aceptar**.

   Kaspersky Embedded Systems Security iniciará la restauración del primero de los objetos seleccionados.

9. Si ya existe un objeto con este nombre en la ubicación especificada, se abrirá la ventana **Ya existe un objeto con este nombre**.

   a. Seleccione una de las siguientes acciones de Kaspersky Embedded Systems Security:

      - **Reemplazar**, para restaurar un objeto en lugar del existente.
      - **Cambiar el nombre**, para guardar un objeto restaurado con otro nombre. En el campo de entrada, introduzca el nombre de archivo del objeto nuevo y la ruta completa a él.
      - **Agregar un sufijo al nombre**: para cambiar el nombre de un objeto al agregar un sufijo al su nombre de archivo. Escriba el sufijo en el campo de entrada.

   b. Si se seleccionan varios objetos para restaurar, a fin de aplicar la acción seleccionada, tal como **Reemplazar** o **Cambiar el nombre** a los objetos seleccionados restantes, seleccione la casilla de verificación **Aplicar a todos los objetos seleccionados**. (Si seleccionó el valor **Cambiar el nombre**, la casilla de verificación **Aplicar a todos los objetos seleccionados** no estará disponible).

   c. Haga clic en **Aceptar**.

   Se restaurará el objeto. En el registro de auditoría del sistema se ingresará información sobre la operación de restauración.

   Si no seleccionó la opción **Aplicar a todos los objetos seleccionados** en la ventana **Restaurar objeto**, la ventana **Restaurar objeto** volverá a abrirse. Mediante esta ventana, puede especificar la ubicación en la que se guardará el objeto seleccionado (vea el paso 4 de este procedimiento).

Cómo mover objetos a Cuarentena

Puede enviar archivos a Cuarentena de forma manual.

► *Para poner un archivo en cuarentena, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Cuarentena**.
2. Seleccione **Agregar**.
3. En la ventana **Abrir**, seleccione el archivo del disco que desea poner en cuarentena.
4. Haga clic en **Aceptar**.

Kaspersky Embedded Systems Security pondrá en cuarentena el archivo seleccionado.

Eliminación de objetos de la cuarentena

De acuerdo a la configuración de la tarea de Análisis de archivos en cuarentena, Kaspersky Embedded Systems Security elimina automáticamente de la carpeta de Cuarentena los objetos cuyo estado haya cambiado a *Infectado* durante el análisis de Cuarentena con las bases de datos actualizadas si Kaspersky Embedded Systems Security no ha podido desinfectarlos. Kaspersky Embedded Systems Security no elimina otros objetos de la Cuarentena.

Es posible eliminar uno o varios objetos de la cuarentena.

► *Para eliminar uno o varios objetos de la cuarentena, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Cuarentena**.
3. Realice uno de los siguientes pasos:
   - Para eliminar un objeto, seleccione **Eliminar** en el menú contextual del nombre del objeto.
   - Para eliminar varios objetos, seleccione los objetos que desea eliminar con las teclas **Ctrl** o **Shift**, abra el menú contextual en cualquiera de los objetos seleccionados y seleccione **Eliminar**.
4. En la ventana de confirmación, haga clic en el botón **Sí** para confirmar la operación.

Los objetos seleccionados se eliminarán de la cuarentena.

Envío de objetos probablemente infectados a Kaspersky Lab para su análisis

Si el comportamiento de un archivo le da motivos para sospechar que contiene una amenaza y Kaspersky Embedded Systems Security considera que dicho archivo está limpio, es posible que se trate de una amenaza desconocida, cuya firma aún no se agregó a las bases de datos. Puede enviar este archivo a Kaspersky Lab para análisis. Los analistas de Anti-Virus de Kaspersky Lab lo analizarán y si detectan una amenaza nueva en él, la agregarán a un registro que la identificará en las bases de datos. Es probable que cuando vuelva a analizar el objeto después de que se haya actualizado la base de datos, Kaspersky Embedded Systems Security considere que este objeto está infectado y lo podrá desinfectar. No solo podrá conservar el objeto, sino también evitará un ataque de virus.

Sólo los archivos en cuarentena se pueden enviar para análisis. Los archivos en cuarentena se almacenan en forma cifrada y no son eliminados por la aplicación antivirus instalada en el servidor de correo durante la transferencia.

No se puede enviar un objeto en cuarentena a Kaspersky Lab para análisis después de que caduca la licencia.

► *Para enviar un archivo para análisis a Kaspersky Lab, siga estos pasos:*

1. Si el archivo no se colocó en cuarentena, en primer lugar, muévalo a **Cuarentena**.
2. En el nodo **Cuarentena**, abra el menú contextual del archivo que desea enviar para análisis y seleccione **Enviar objeto a analizar** en el menú contextual.
3. En la ventana de confirmación que se abre, haga clic en **Sí** si está seguro de que desea enviar el objeto seleccionado a análisis.
4. Si un cliente de correo está configurado en el equipo en que está instalada la consola de la aplicación, se crea un nuevo mensaje de correo electrónico. Revíselo y haga clic en el botón **Enviar**.

   El campo **Destinatario** contiene la dirección de correo electrónico de Kaspersky Lab newvirus@kaspersky.com. El campo Asunto contendrá el texto "Objeto en cuarentena".

   El cuerpo del mensaje incluirá la línea siguiente: “Este archivo se enviará a Kaspersky Lab para análisis”. Cualquier información adicional sobre el archivo, por qué se consideró probablemente infectado o peligroso, cómo se comporta o cómo afecta el sistema puede incluirse en el cuerpo del mensaje.

   El archivo de almacenamiento <nombre de objeto>.cab se adjuntará al mensaje. Este archivo de almacenamiento contendrá el archivo <uuid>.klq con el objeto en forma cifrada y el archivo <uuid>.txt con

información sobre el objeto extraído por Kaspersky Embedded Systems Security, además del archivo Sysinfo.txt, que contiene la información siguiente sobre Kaspersky Embedded Systems Security y el sistema operativo instalado en el equipo:

- Nombre y versión del sistema operativo.
- Nombre y versión de Kaspersky Embedded Systems Security.
- Fecha de lanzamiento de la última actualización de bases de datos instalada.
- Clave activa.

Los analistas de Anti-Virus de Kaspersky Lab necesitan esta información para poder analizar su archivo de manera más rápida y eficaz. Sin embargo, si no desea transferir esta información, puede eliminar el archivo Sysinfo.txt del archivo de almacenamiento.

Si un cliente de correo no está instalado en el equipo con la Consola de la aplicación, la aplicación le solicita guardar el objeto cifrado seleccionado en el archivo. Este archivo se puede enviar a Kaspersky Lab en forma manual.

► *Para guardar un objeto cifrado en un archivo, siga estos pasos:*

1. En la ventana que se abre con una solicitud para guardar el objeto, haga clic en **Aceptar**.
2. Seleccione una carpeta en la unidad del equipo protegido o una carpeta de red en la que se guardará el archivo que contiene el objeto.

El objeto se guardará en un archivo CAB.

Configuración de las opciones de la Cuarentena

Puede configurar las opciones de la cuarentena. La nueva configuración de la Cuarentena se aplica inmediatamente después de guardar las opciones.

► *Para configurar los valores de la Cuarentena, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Abra el menú contextual en el nodo secundario **Cuarentena**.
3. Seleccione **Propiedades**.
4. En la ventana **Propiedades de la Cuarentena**, configure las opciones de la cuarentena necesarias según sus requisitos:
   - En la sección **Configuración de Cuarentena**:
     - **Carpeta de cuarentena**

       Ruta a la Carpeta de cuarentena en formato UNC (convención de nomenclatura universal).

       La ruta predeterminada es C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Quarantine\.

     - **Tamaño máximo de cuarentena**

       Esta casilla de verificación habilita o deshabilita la función que supervisa el tamaño total de objetos almacenados en la carpeta de Cuarentena. Si se supera el valor especificado (el valor predeterminado es 200 MB), Kaspersky Embedded Systems Security registra el evento *Se superó el tamaño máximo de la Cuarentena* y emite una notificación según la

configuración para notificaciones sobre eventos de este tipo.

Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security supervisa el tamaño total de objetos colocados en Cuarentena.

Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no supervisa el tamaño total de objetos colocados en Cuarentena.

De forma predeterminada, la casilla está desactivada.

- **Valor umbral de espacio disponible**

Si el tamaño de los objetos en la Cuarentena supera el tamaño máximo de Cuarentena o supera el umbral del espacio disponible, Kaspersky Embedded Systems Security le notificará sobre esto y, al mismo tiempo, continuará colocando objetos en la Cuarentena.

- En la sección **Configuración de restauración**:
  - **Carpeta de destino para restaurar objetos**

5. Haga clic en **Aceptar**.

Se guardará la configuración reciente para la Cuarentena.

Estadísticas de cuarentena

Se puede visualizar información sobre la cantidad de objetos en cuarentena: estadísticas de cuarentena.

► *Para ver las estadísticas de cuarentena,*

abra el menú contextual en el nodo **Cuarentena** en el árbol de la Consola de la aplicación y seleccione **Estadísticas**.

La ventana **Estadísticas** muestra información sobre la cantidad de objetos almacenados en Cuarentena (consulte la tabla a continuación):

Campo	Descripción
Objetos probablemente infectados	Cantidad de objetos probablemente infectados encontrados por Kaspersky Embedded Systems Security.
Espacio de Cuarentena utilizado	Tamaño total de datos en la carpeta de Cuarentena.
Falsas alarmas	La cantidad de objetos que recibieron el estado *Falsa alarma* debido a que se clasificaron como no infectados durante el análisis de archivos en cuarentena con las bases de datos actualizadas.
Objetos desinfectados	La cantidad de objetos que recibieron el estado *Desinfectados* después del análisis de archivos en cuarentena.
Número total de objetos	Cantidad total de objetos en cuarentena.

Creación de copias de seguridad de los objetos. Copia de seguridad

Esta sección brinda información sobre las copias de seguridad de los objetos maliciosos detectados antes de la

desinfección o la eliminación, así como instrucciones para configurar las Copia de seguridad.

En esta sección

Acerca de la copia de seguridad de objetos antes de la desinfección o eliminación

Kaspersky Embedded Systems Security almacena copias cifradas de los objetos clasificados como *Infectados* en *Copia de seguridad* antes de desinfectarlos o eliminarlos.

Si el objeto forma parte de un objeto compuesto (por ejemplo, parte de un archivo de almacenamiento), Kaspersky Embedded Systems Security guardará dicho objeto compuesto en su totalidad en Copia de seguridad. Por ejemplo, si Kaspersky Embedded Systems Security ha detectado que uno de los objetos de una base de datos de correo está infectado, hará una copia de seguridad de toda la base de datos de correo.

Los objetos grandes ubicados en Copia de seguridad por Kaspersky Embedded Systems Security pueden ralentizar el sistema y reducir el espacio en el disco duro.

Los archivos se pueden restaurar de las Copia de seguridad a su carpeta original o a una carpeta diferente en el equipo protegido o en otro equipo de la red de área local. Un archivo se puede restaurar desde Copia de seguridad, por ejemplo, si un archivo infectado contenía información importante, pero durante la desinfección de este archivo Kaspersky Embedded Systems Security y no pudo mantener su integridad y, por lo tanto, la información ya no está disponible.

Restaurar archivos de la copia de seguridad puede producir la infección del equipo.

Visualización de objetos almacenados en Copia de seguridad

Los objetos se pueden almacenar en la carpeta de Copia de seguridad solo mediante la Consola de la aplicación en el nodo **Copia de seguridad**. No se pueden visualizar mediante los administradores de archivos de Microsoft Windows.

► *Para ver los archivos en las Copia de seguridad,*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Copia de seguridad**.

   La información sobre los objetos colocados en las Copia de seguridad se muestra en el panel de detalles del nodo seleccionado.

► *Para encontrar el objeto necesario en la lista de Objetos en Copia de seguridad,*

ordene los objetos o filtre los objetos.

En esta sección

Cómo ordenar archivos en Copia de seguridad

De manera predeterminada, los archivos en copia de seguridad se ordenan por la fecha de guardado en orden cronológico inverso. Para buscar el archivo requerido, puede ordenar los archivos de acuerdo con el contenido de cualquiera de las columnas en el panel de detalles.

Los resultados ordenados se guardarán si cierra y vuelve a abrir el nodo **Copia de seguridad** o si cierra la Consola de la aplicación, guarda el archivo msc y vuelve a abrirlo desde este archivo.

► *Para ordenar los archivos en copia de seguridad, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Copia de seguridad**.
3. En la lista de archivos en **Copia de seguridad**, seleccione el encabezado de la columna que desea usar para ordenar los objetos.

Los archivos en las Copia de seguridad se ordenarán según el criterio seleccionado.

Filtrado de archivos en Copia de seguridad

Para buscar el archivo requerido en Copia de seguridad, puede filtrar los archivos: mostrar en el nodo **Copia de seguridad** solo los archivos que satisfagan los criterios de filtrado (filtros) que haya especificado.

El resultado de la clasificación se guardará si usted cierra y vuelve a abrir el nodo **Copia de seguridad** o si cierra la Consola de la aplicación, guarda el archivo msc y vuelve a abrirla desde este archivo.

► *Para filtrar los archivos en Copia de seguridad, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Copia de seguridad** y seleccione **Filtrar**.

   Se abre la ventana **Configuración de filtro**.
2. Para agregar un filtro, siga estos pasos:
   a. De la lista **Nombre del campo**, seleccione el campo con cuyos valores se compararán los valores de filtro durante la selección.
   b. En la lista **Operador**, seleccione la condición de filtrado. Los valores de las condiciones de filtrado en la lista pueden diferir según el valor que haya seleccionado en el campo **Nombre del campo**.
   c. Introduzca el valor de filtro en el campo **Valor del campo** o selecciónelo.
   d. Haga clic en el botón **Agregar**.

El filtro que agregó aparecerá en la lista de filtros en la ventana **Configuración de filtro**. Repita estos pasos para cada filtro que agregue. Se pueden usar las siguientes directrices mientras se trabaja con los filtros:

- Para combinar varios filtros mediante el operador lógico "AND", seleccione **Si se cumplen todas las condiciones**.
- Para combinar varios filtros mediante el operador lógico "OR", seleccione **Si se cumple alguna condición**.
- Para eliminar un filtro, seleccione el filtro que desea eliminar en la lista de filtros y haga clic en el botón **Eliminar**.
- Para editar un filtro, selecciónelo de la lista de filtros en la ventana **Configuración de filtro**, modifique los valores requeridos en el campo **Nombre del campo**, **Operador** o **Valor del campo** y haga clic en el botón **Reemplazar**.

Una vez agregados todos los filtros, haga clic en el botón **Aplicar**. Sólo los archivos seleccionados por los filtros especificados se mostrarán en la lista.

► *Para mostrar todos los archivos incluidos en la lista de objetos almacenados en Copia de seguridad*

seleccione **Eliminar filtro** en el menú contextual del nodo **Copia de seguridad**.

Restauración de archivos de Copia de seguridad

Kaspersky Embedded Systems Security almacena archivos en la carpeta Copia de seguridad en forma cifrada con el fin de proteger el equipo protegido de cualquier efecto peligroso posible.

Se puede restaurar cualquier archivo de la copia de seguridad.

Es posible que se deba restaurar un archivo en los casos siguientes:

- Si el archivo original, que parecía estar infectado, contenía información importante y Kaspersky Embedded Systems Security no pudo mantener su integridad, como resultado, la información contenida en el archivo dejó de estar disponible.
- Si considera que el archivo no es peligroso para el equipo y desea utilizarlo. Si no desea que Kaspersky Embedded Systems Security considere a este archivo infectado o probablemente infectado durante los análisis subsiguientes, puede excluirlo del procesamiento en la tarea de Protección de archivos en tiempo real y en las tareas de Análisis a pedido. Para ello, especifique el archivo como la configuración **Excluir archivos** o como la configuración **No detectar** en las tareas correspondientes.

Restaurar archivos de la copia de seguridad puede producir la infección del equipo.

Al restaurar un archivo, puede seleccionar dónde se guardará: ubicación original (de manera predeterminada), carpeta especial para objetos restaurados en el equipo protegido o carpeta personalizada en el equipo en que está instalada la Consola de la aplicación, o bien en otro equipo de la red.

Restaurar a carpeta se utiliza para almacenar objetos restaurados en el equipo protegido. Puede configurar los valores de seguridad especiales para que se realice su análisis. La Configuración de Copia de seguridad especifica la ruta de acceso a esta carpeta (consulte la sección “Configuración de las opciones de Copia de seguridad”, en la página 195).

De manera predeterminada, cuando Kaspersky Embedded Systems Security restaura un archivo hace una copia de él en Copia de seguridad. La copia del archivo se puede eliminar de la copia de seguridad una vez restaurado.

► *Para restaurar los archivos de Copia de seguridad, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Copia de seguridad**.
3. En el panel de detalles del nodo **Copia de seguridad**, realice una de las siguientes acciones:
   - Para restaurar un objeto, seleccione **Restaurar** desde el menú contextual del objeto que desea restaurar.
   - Para restaurar varios objetos, seleccione los objetos que desea restaurar mediante la tecla **CTRL** o **MAYÚS**, haga clic con el botón secundario en uno de los objetos seleccionados y seleccione **Restaurar** en el menú contextual.

   Se abre la ventana **Restaurar objeto**.
4. En la ventana **Restaurar objeto**, especifique la carpeta donde se guardará el objeto que se está restaurando para cada objeto seleccionado.

   El nombre del objeto restaurado se muestra en el campo **Objeto** en la parte superior de la ventana. Si selecciona varios objetos, se mostrará el nombre del primer objeto en la lista de objetos seleccionados.
5. Realice uno de los siguientes pasos:
   - Para restaurar un objeto a su ubicación original, seleccione **Restaurar a la carpeta de origen**.
   - Para restaurar un objeto a la carpeta especificada como la ubicación para los objetos restaurados en la configuración, seleccione **Restaurar a la carpeta de restauración predeterminada**.
   - Para guardar un objeto en una carpeta diferente en el equipo en que está instalada la Consola de la aplicación o en una carpeta compartida, seleccione **Restaurar a una carpeta del equipo local o de un recurso de red** y, a continuación, seleccione la carpeta necesaria o especifique una ruta a esta.
6. Si no desea guardar una copia del archivo en la carpeta Copia de seguridad después de restaurarlo, seleccione la casilla de verificación **Eliminar objetos del depósito una vez restaurados** (de manera predeterminada, esta casilla de verificación está desactivada).
7. Para aplicar las condiciones de restauración especificadas en los restantes objetos seleccionados, active la casilla de verificación **Aplicar a todos los objetos seleccionados**.

   Todos los objetos seleccionados se restaurarán y se guardarán en la ubicación especificada: si seleccionó **Restaurar a la carpeta de origen**, cada uno de los objetos se guardará en su ubicación original; si seleccionó **Restaurar a la carpeta de restauración predeterminada** o **Restaurar a una carpeta del equipo local o de un recurso de red**, todos los objetos se guardarán en la carpeta especificada.
8. Haga clic en **Aceptar**.

   Kaspersky Embedded Systems Security iniciará la restauración del primero de los objetos seleccionados.
9. Si ya existe un objeto con este nombre en la ubicación especificada, se abrirá la ventana **Ya existe un objeto con este nombre**.

   a. Seleccione una de las siguientes acciones de Kaspersky Embedded Systems Security:
      - **Reemplazar**, para restaurar un objeto en lugar del existente.
      - **Cambiar el nombre**, para guardar un objeto restaurado con otro nombre. En el campo de entrada, introduzca el nombre de archivo del objeto nuevo y la ruta completa a él.
      - **Agregar un sufijo al nombre**: para cambiar el nombre de un objeto al agregar un sufijo al su

nombre de archivo. Escriba el sufijo en el campo de entrada.

b. Si se seleccionan varios objetos para restaurar, a fin de aplicar la acción seleccionada, tal como **Reemplazar** o **Cambiar el nombre** a los objetos seleccionados restantes, seleccione la casilla de verificación **Aplicar a todos los objetos seleccionados**. (Si seleccionó el valor **Cambiar el nombre**, la casilla de verificación **Aplicar a todos los objetos seleccionados** no estará disponible).

c. Haga clic en **Aceptar**.

Se restaurará el objeto. En el registro de auditoría del sistema se ingresará información sobre la operación de restauración.

Si no seleccionó la opción **Aplicar a todos los objetos seleccionados** en la ventana **Restaurar objeto**, la ventana **Restaurar objeto** volverá a abrirse. Mediante esta ventana, puede especificar la ubicación en la que se guardará el objeto seleccionado (vea el paso 4 de este procedimiento).

Eliminación de archivos de Copia de seguridad

► *Para eliminar uno o varios archivos de la copia de seguridad, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Seleccione el nodo secundario **Copia de seguridad**.
3. Realice uno de los siguientes pasos:
   - Para eliminar un objeto, seleccione **Eliminar** en el menú contextual del nombre del objeto.
   - Para eliminar varios objetos, seleccione los objetos que desea eliminar con las teclas **Ctrl** o **Shift**, abra el menú contextual en cualquiera de los objetos seleccionados y seleccione **Eliminar**.
4. En la ventana de confirmación, haga clic en el botón **Sí** para confirmar la operación.

Los archivos seleccionados se eliminarán de las Copia de seguridad.

Configuración de Copia de seguridad

► *Para configurar los valores de Copia de seguridad, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Depósitos**.
2. Abra el menú contextual en el nodo **Copia de seguridad**.
3. Seleccione **Propiedades**.
4. En la ventana **Propiedades de Copia de seguridad**, configure las opciones de Copia de seguridad necesarias según sus requisitos:

   En la sección **Configuración de Copia de seguridad**:

   - **Carpeta de Copia de seguridad**

     Ruta a la Carpeta de copia de seguridad en formato UNC (convención de nomenclatura universal).

     La ruta predeterminada es C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Backup\.

   - **Tamaño máx. de Copia de seguridad (MB)**

     Esta casilla de verificación habilita o deshabilita la función que supervisa el tamaño total de objetos almacenados en la carpeta Copia de seguridad. Si se supera el valor

especificado (el valor predeterminado es 200 MB), Kaspersky Embedded Systems Security registra el evento *Se superó el tamaño máximo de Copia de seguridad* y emite una notificación según la configuración para notificaciones sobre eventos de este tipo.

Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security supervisa el tamaño total de objetos colocados en Copia de seguridad.

Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no supervisa el tamaño total de objetos colocados en Copia de seguridad.

De forma predeterminada, la casilla está desactivada.

- **Valor umbral de espacio disponible (MB)**

  La casilla de verificación habilita o deshabilita la función que supervisa la cantidad mínima de espacio libre en Copia de seguridad (el valor predeterminado es 50 MB). Si la cantidad de espacio libre disminuye por debajo del umbral especificado, Kaspersky Embedded Systems Security registra el evento *Se superó el umbral de espacio disponible para Copia de seguridad* y emite una notificación según la configuración para notificaciones sobre eventos de este tipo.

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security supervisa la cantidad de espacio libre en Copia de seguridad.

  La casilla de verificación Valor umbral de espacio disponible (MB) está activa si la casilla de verificación Tamaño máx. de Copia de seguridad (MB) está seleccionada.

  De forma predeterminada, la casilla está activada.

Si el tamaño de los objetos en Copia de seguridad supera el tamaño máximo de Copia de seguridad o supera el umbral del espacio disponible, Kaspersky Embedded Systems Security le notificará sobre esto y, al mismo tiempo, continuará colocando objetos en Copia de seguridad.

En la sección **Configuración de restauración**:

- **Carpeta de destino para restaurar objetos**

  Ruta a la carpeta para la restauración de objetos en formato UNC (convención de nomenclatura universal).

  Ruta predeterminada: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored\.

5. Haga clic en **Aceptar**.

Se guarda la configuración de Copia de seguridad.

Estadísticas de Copia de seguridad

Puede visualizar la información sobre el estado actual de la copia de seguridad: Estadísticas de Copia de seguridad.

► *Para ver las estadísticas de Copia de seguridad,*

abra el menú contextual en el nodo **Copia de seguridad** en el árbol de la Consola de la aplicación y seleccione **Estadísticas**. Se abre la ventana **Estadísticas de Copia de seguridad**.

La ventana **Estadísticas de Copia de seguridad** muestra información sobre el estado actual de las Copia de seguridad (consulte la tabla a continuación).

Tabla 35. Información sobre el estado actual de la copia de seguridad

Campo	Descripción
Tamaño actual de Copia de seguridad	Tamaño de datos en la carpeta Copia de seguridad; la aplicación calcula el tamaño del archivo en forma cifrada.
Número total de objetos	Cantidad total actual de objetos en la copia de seguridad

Registro de eventos. Registros de Kaspersky Embedded Systems Security

Esta sección proporciona información sobre el funcionamiento de los registros de Kaspersky Embedded Systems Security: el registro de auditoría del sistema, los registros de ejecución de tareas y el registro de eventos.

En este capítulo

Modos de registrar eventos de Kaspersky Embedded Systems Security

Los eventos de Kaspersky Embedded Systems Security se dividen en dos grupos:

- Eventos relacionados con el procesamiento de objetos en las tareas de Kaspersky Embedded Systems Security.
- Eventos relacionados con la administración de Kaspersky Embedded Systems Security, como el inicio de la aplicación, la creación o la eliminación de tareas, o la edición de la configuración de tareas.

Kaspersky Embedded Systems Security utiliza los siguientes métodos para registrar eventos:

- **Registros de tareas**. Un registro de tareas contiene información sobre el estado actual de las tareas y los eventos que ocurrieron durante su ejecución.
- **Registro de auditoría del sistema**. El registro de auditoría del sistema contiene información sobre los eventos que están relacionados con la administración de Kaspersky Embedded Systems Security.
- **Registro de eventos**. El registro de eventos contiene información sobre los eventos que se requieren para el diagnóstico de fallas en el funcionamiento de Kaspersky Embedded Systems Security. El registro de eventos está disponible en el Visor de eventos de Microsoft Windows.
- **Registro de seguridad**. El registro de seguridad contiene información sobre eventos asociados con la

violación de la seguridad o intentaron hacerlo en el equipo protegido.

Si ocurre un problema durante el funcionamiento de Kaspersky Embedded Systems Security (por ejemplo, Kaspersky Embedded Systems Security o una tarea individual se interrumpe de manera anormal o no se inicia), puede crear un archivo de rastreo y volcado de memoria de procesos de Kaspersky Embedded Systems Security y enviar los archivos con esta información para análisis al soporte técnico de Kaspersky Lab, con el fin de diagnosticar el problema ocurrido.

Kaspersky Embedded Systems Security no envía ningún archivo de volcado o rastreo automáticamente. Solo los usuarios con los permisos correspondientes pueden enviar datos de diagnóstico.

Kaspersky Embedded Systems Security escribe la información en los archivos de seguimiento y el archivo de volcado de memoria en formato no cifrado. El usuario selecciona la carpeta donde se guardan los archivos, que es administrada por la configuración del sistema operativo y la configuración de Kaspersky Embedded Systems Security. Puede configurar permisos de acceso (consulte la sección “Administración de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security” en la página 220) para permitir el acceso a registros, archivos de volcado y rastreo solo a usuarios requeridos.

Registro de auditoría del sistema

Kaspersky Embedded Systems Security realiza la auditoría del sistema de los eventos relacionados con la administración de Kaspersky Embedded Systems Security. La aplicación registra información sobre, por ejemplo, el inicio de la aplicación, los inicios y las detenciones de las tareas de Kaspersky Embedded Systems Security, los cambios en la configuración de tareas y la creación y eliminación de tareas de Análisis a pedido. Los registros de todos esos eventos se muestran en el panel de resultados cuando se selecciona el nodo **Registro de auditoría del sistema** en la Consola de la aplicación.

De manera predeterminada, Kaspersky Embedded Systems Security almacena registros en el registro de auditoría del sistema durante un periodo indeterminado. Se puede especificar el periodo de almacenamiento para los registros del registro de auditoría del sistema.

Puede especificar una carpeta que Kaspersky Embedded Systems Security usará para almacenar los archivos que contienen el registro de auditoría del sistema que no sea la predeterminada.

En esta sección

Cómo ordenar eventos en el registro de auditoría del sistema

De manera predeterminada, los eventos en el nodo registro de auditoría del sistema se muestran en orden cronológico inverso.

Los eventos se pueden ordenar por los contenidos de cualquier columna, excepto la columna **Evento**.

► *Para ordenar eventos en el registro de auditoría del sistema:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Seleccione el nodo secundario **Registro de auditoría del sistema**.
3. En el panel de detalles, seleccione el encabezado de columna que desea usar para ordenar los eventos en la lista.

Los resultados ordenados se guardarán hasta su próxima sesión de visualización en el registro de auditoría del sistema.

Filtrado de eventos en el registro de auditoría del sistema

Puede configurar el registro de auditoría del sistema para que muestre solo los registros de eventos que cumplen con las condiciones de filtrado (filtros) que ha especificado.

► *Para filtrar eventos del registro de auditoría del sistema, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Abra el menú contextual del nodo secundario **Registro de auditoría del sistema** y seleccione **Filtrar**.

   Se abre la ventana **Configuración de filtro**.
3. Para agregar un filtro, siga estos pasos:
   a. En la lista **Nombre del campo**, seleccione una columna por la que se filtrarán los eventos.
   b. En la lista **Operador**, seleccione la condición de filtrado. Las condiciones de filtrado varían según el elemento seleccionado en la lista **Nombre del campo**.
   c. En la lista **Valor del campo**, seleccione un valor para el filtro.
   d. Haga clic en el botón **Agregar**.

      El filtro que agregó aparecerá en la lista de filtros en la ventana **Configuración de filtro**.
4. Si es necesario, realice una de las siguientes acciones:
   - Si desea combinar varios filtros mediante el operador lógico “AND”, seleccione **Si se cumplen todas las condiciones**.
   - Si desea combinar varios filtros mediante el operador lógico “OR”, seleccione **Si se cumple alguna condición**.
5. Haga clic en el botón **Aplicar** para guardar las condiciones de filtrado en el registro de auditoría del sistema.

   La lista de eventos del registro de auditoría del sistema muestra solo los eventos que cumplen las condiciones de filtrado. Los resultados del filtrado se guardarán hasta su próxima sesión de visualización en el registro de auditoría del sistema.

► *Para deshabilitar el filtro:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Abra el menú contextual del nodo secundario **Registro de auditoría del sistema** y seleccione **Eliminar filtro**.

   La lista de eventos del registro de auditoría del sistema mostrará todos los eventos.

Eliminar eventos del registro de auditoría del sistema

De manera predeterminada, Kaspersky Embedded Systems Security almacena registros en el registro de auditoría del sistema durante un periodo indeterminado. Se puede especificar el periodo de almacenamiento para los registros del registro de auditoría del sistema.

Se pueden eliminar manualmente todos los eventos del registro de auditoría del sistema.

► *Para eliminar eventos del registro de auditoría del sistema:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Abra el menú contextual del nodo secundario **Registro de auditoría del sistema** y seleccione **Eliminar**.
3. Realice uno de los siguientes pasos:
   - Si desea guardar el contenido del registro como un archivo de formato CSV o TXT antes de eliminar los eventos del registro de auditoría del sistema, haga clic en el botón **Sí** en la ventana de confirmación de eliminación. En la ventana que se abre, especifique el nombre y la ubicación del archivo.
   - Si no desea guardar el contenido del registro como un archivo, haga clic en el botón **No** en la ventana de confirmación de eliminación.

Se borrará el registro de auditoría del sistema.

Registros de tareas

Esta sección proporciona información acerca de los registros de tareas de Kaspersky Embedded Systems Security e instrucciones sobre cómo administrarlos.

En esta sección

Acerca de los registros de tareas

La información sobre la ejecución de las tareas de Kaspersky Embedded Systems Security se muestra en el panel de detalles cuando se selecciona el nodo **Registros de tareas** en la Consola de la aplicación.

En el registro de cada tarea, puede ver las estadísticas de la ejecución de la tarea, los detalles de cada uno de los objetos que han sido procesados por la aplicación desde el inicio de la tarea hasta ese momento y la configuración

de esta.

De forma predeterminada, Kaspersky Embedded Systems Security almacena registros de tareas durante 30 días desde la finalización de la tarea. Se puede cambiar el periodo de almacenamiento para los eventos del registro de tarea.

Puede especificar una carpeta diferente de la predeterminada para que Kaspersky Embedded Systems Security almacene los archivos que contienen los registros de tareas. También puede seleccionar los eventos que Kaspersky Embedded Systems Security asentará en los registros de tareas.

Visualización de la lista de eventos en los registros de tarea

► *Para ver la lista de eventos en los registros de tarea:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Seleccione el subnodo **Registros de tareas**.

   En el panel de detalles, aparecerá la lista de los eventos guardados en los registros de tareas de Kaspersky Embedded Systems Security.

Los eventos se pueden ordenar por cualquier columna o filtrar.

Cómo ordenar los eventos en los registros de tareas

De manera predeterminada, los eventos en los registros de tarea se muestran en orden cronológico inverso. Se pueden ordenar por cualquier columna.

► *Para ordenar eventos en los registros de tarea:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Seleccione el subnodo **Registros de tareas**.
3. En el panel de resultados, seleccione el encabezado de la columna que desea usar para ordenar los eventos en los registros de tareas de Kaspersky Embedded Systems Security.

   Los resultados ordenados se guardarán hasta su próxima sesión de visualización en los registros de tarea.

Filtrado de eventos en los registros de tareas

Puede configurar la lista de registros de tarea para que muestren únicamente los registros de eventos que cumplan con las condiciones de filtrado (filtros) que especificó.

► *Para filtrar eventos en los registros de tareas:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Abra el menú contextual del nodo secundario **Registros de tareas** y seleccione **Filtrar**.

   Se abre la ventana **Configuración de filtro**.
3. Para agregar un filtro, siga estos pasos:
   a. En la lista **Nombre del campo**, seleccione una columna por la que se filtrarán los eventos.
   b. En la lista **Operador**, seleccione la condición de filtrado. Las condiciones de filtrado varían según el

elemento seleccionado en la lista **Nombre del campo**.

c. En la lista **Valor del campo**, seleccione un valor para el filtro.

d. Haga clic en el botón **Agregar**.

El filtro que agregó aparecerá en la lista de filtros en la ventana **Configuración de filtro**.

4. Si es necesario, realice una de las siguientes acciones:
   - Si desea combinar varios filtros mediante el operador lógico “AND”, seleccione **Si se cumplen todas las condiciones**.
   - Si desea combinar varios filtros mediante el operador lógico “OR”, seleccione **Si se cumple alguna condición**.
5. Haga clic en el botón **Aplicar** para guardar las condiciones de filtrado en la lista de registros de tarea.

La lista de eventos de registros de tarea muestra solo los eventos que cumplen con las condiciones de filtrado. Los resultados filtrados se guardarán hasta su próxima sesión de visualización en los registros de tarea.

► *Para deshabilitar el filtro:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Abra el menú contextual del nodo secundario **Registros de tareas** y seleccione **Eliminar filtro**.

En consecuencia, la lista de eventos de los registros de tarea mostrará todos los eventos.

Visualización de las estadísticas y la información acerca de una tarea de Kaspersky Embedded Systems Security en los registros de tareas

En los registros de tarea, puede ver información detallada sobre todos los eventos que han ocurrido en las tareas desde que se iniciaron hasta ese momento, así como las estadísticas de ejecución de las tareas y la configuración de las tareas.

► *Para ver las estadísticas y la información acerca de una tarea de Kaspersky Embedded Systems Security:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Seleccione el subnodo **Registros de tareas**.
3. En el panel de resultados, abra la ventana **Registros** mediante uno de los siguientes métodos:
   - Con un doble clic en el evento que se ha producido en la tarea de la que desea ver el registro.
   - Abra el menú contextual del evento que se ha producido en la tarea de la que desea ver el registro y seleccione **Ver registro**.
4. En la ventana que se abre, se muestra la siguiente información:
   - La pestaña **Estadísticas** muestra la hora de inicio y finalización de la tarea, así como las estadísticas de la tarea.
   - La ficha **Eventos** muestra una lista de eventos que se registraron durante la ejecución de la tarea.
   - La pestaña **Opciones** muestra la configuración de la tarea.
5. Si es necesario, haga clic en el botón **Filtrar** para filtrar los eventos en el registro de tareas.
6. Si es necesario, haga clic en el botón **Exportar** para exportar los datos desde el registro de tareas a un archivo con formato TXT o CSV.

7. Presione el botón **Cerrar**.

Se cerrará la ventana **Registros**.

Exportación de la información desde un registro de tareas

Puede exportar los datos de un registro de tareas a un archivo con formato TXT o CSV.

► *Para exportar datos desde un registro de tareas:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Seleccione el subnodo **Registros de tareas**.
3. En el panel de resultados, abra la ventana **Registros** mediante uno de los siguientes métodos:
   - Con un doble clic en el evento que se ha producido en la tarea de la que desea ver el registro.
   - Abra el menú contextual del evento que se ha producido en la tarea de la que desea ver el registro y seleccione **Ver registro**.
4. En la parte inferior de la ventana **Registros**, haga clic en el botón **Exportar**.

   Se abre la ventana **Guardar como**.
5. Especifique el nombre, la ubicación, el tipo y la codificación del archivo al que desea exportar los datos del registro de tareas.
6. Haga clic en el botón **Guardar**.

Se guarda la configuración especificada.

Eliminación de eventos de los registros de tareas

De forma predeterminada, Kaspersky Embedded Systems Security almacena registros de tareas durante 30 días desde la finalización de la tarea. Se puede cambiar el periodo de almacenamiento para los eventos del registro de tarea.

Se pueden eliminar manualmente todos los eventos de los registros de las tareas que ya se han completado hasta ese momento.

No se eliminarán los eventos de los registros de las tareas que se están ejecutando ni las tareas que están utilizando otros usuarios.

► *Para eliminar los eventos de los registros de tarea:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Registros y notificaciones**.
2. Seleccione el subnodo **Registros de tareas**.
3. Realice uno de los siguientes pasos:
   - Si desea eliminar los eventos de los registros de todas las tareas que ya se han completado hasta ese momento, abra el menú contextual del nodo secundario **Registros de tareas** y seleccione **Eliminar**.
   - Si desea borrar el registro de una tarea individual, en el panel de detalles, abra el menú contextual de

un evento que se ha producido en la tarea de la que desea borrar el registro y seleccione **Eliminar**.

- Si desea borrar los registros de varias tareas:

  a. En el panel de detalles, use las teclas **Ctrl** o la de **Mayús** para seleccionar los eventos que han ocurrido en las tareas de las que desea borrar los registros.

  b. Abra el menú contextual de cualquier evento seleccionado y seleccione **Eliminar**.

4. Haga clic en el botón **Sí** de la ventana de confirmación de eliminación para confirmar que desea eliminar los registros.

Se borrarán los registros de las tareas que ha seleccionado. La eliminación de los eventos de los registros de tarea se asentará en el registro de auditoría del sistema.

Registro de seguridad

Kaspersky Embedded Systems Security mantiene un registro de eventos asociados con la violación de la seguridad o los intentos de violación de la seguridad en el equipo protegido. Los siguientes eventos se incluyen en este registro:

- Eventos de Prevención de exploits.
- Eventos de inspección de registros críticos
- Los eventos críticos que indican un intento de violación de la seguridad (para la Protección del equipo en tiempo real, el Análisis a pedido, el Monitor de integridad de archivos, el Control de inicio de aplicaciones y las tareas de Control de dispositivos).

Puede cancelar la selección del registro de seguridad, al igual que el Registro de auditoría del sistema (consulte la sección “Eliminación de eventos del registro de auditoría del sistema”, en la página 200). Además, Kaspersky Embedded Systems Security registra eventos de auditoría del sistema relacionados con el borrado del registro de seguridad.

Visualización del registro de eventos de Kaspersky Embedded Systems Security en el Visor de eventos

Puede ver el registro del evento de Kaspersky Embedded Systems Security con el complemento Visor de eventos de Microsoft Windows para Microsoft Management Console. El registro contiene eventos registrados por Kaspersky Embedded Systems Security, necesarios para el diagnóstico de fallas de su funcionamiento.

Se pueden seleccionar los eventos que se registrarán en el registro de eventos en función de los siguientes criterios:

- **Por tipos de evento.**
- **por nivel de detalle**. El nivel de detalle corresponde al nivel de importancia de los eventos registrados en el registro (eventos informativos, importantes o críticos). El nivel más detallado es el nivel Eventos informativos, que registra todos los eventos y el menos detallado es el nivel Eventos críticos, que registra los eventos críticos únicamente. De manera predeterminada, todos los componentes, excepto el componente Actualización, tienen seleccionado el nivel de detalle Eventos importantes (solo se registran los eventos importantes y críticos); para el componente Actualización, está seleccionado el nivel Eventos informativos.

► *Para consultar el registro del evento de Kaspersky Embedded Systems Security:*

1. Haga clic en el botón **Inicio**, introduzca el comando `mmc` en la barra de búsqueda y presione **INTRO**.

   Se abre la ventana de Microsoft Management Console.

2. Seleccione **Archivo** > **Agregar o eliminar complemento**.

   Se abre la ventana **Agregar o eliminar complementos**.

3. En la lista de complementos disponibles, seleccione el complemento **Visor de eventos** y haga clic en el botón **Agregar**.

   Se abre la ventana **Seleccionar equipo**.

4. En la ventana **Seleccionar equipo**, especifique el equipo en el cual Kaspersky Embedded Systems Security está instalado y haga clic en **Aceptar**.

5. En la ventana **Agregar y eliminar complementos**, haga clic en **Aceptar**.

   En el árbol de Microsoft Management Console, aparece el nodo **Visor de eventos**.

6. Expanda el nodo **Visor de eventos** y seleccione el nodo secundario **Registros de aplicaciones y servicios** > **Kaspersky Embedded Systems Security**.

Se abre el registro del evento de Kaspersky Embedded Systems Security.

Configuración del registro en la Consola de Kaspersky Embedded Systems Security

Puede editar la siguiente configuración de registros de Kaspersky Embedded Systems Security:

- Duración del periodo de almacenamiento para los eventos en los registros de tarea y el registro de auditoría del sistema.
- Ubicación de la carpeta en la que Kaspersky Embedded Systems Security almacena archivos de registros de tareas y el registro de auditoría del sistema.
- Umbrales de generación de los eventos para *La base de datos de la aplicación está desactualizada*, *La base de datos de la aplicación es obsoleta* y *Hace mucho tiempo que no se realiza un análisis de áreas críticas*.
- Eventos que Kaspersky Embedded Systems Security guarda en los registros de tareas, el registro de auditoría del sistema y el registro de eventos de Kaspersky Embedded Systems Security en el Visor de eventos.
- Ajustes para publicar eventos de auditoría y eventos de desempeño de la tarea en el servidor syslog a través del protocolo de syslog.

► *Para configurar los registros de Kaspersky Embedded Systems Security, realice los siguientes pasos:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Registros y notificaciones** y seleccione **Propiedades**.

   Se abre la ventana **Configuración de registros y notificaciones**.

2. En la ventana **Configuración de registros y notificaciones**, configure los registros de acuerdo con sus requisitos. Para ello, realice las siguientes acciones:

   - En la pestaña **General**, de ser necesario, seleccione eventos que Kaspersky Embedded Systems Security guardará en los registros de tareas, el registro de auditoría del sistema y el registro de eventos de Kaspersky Embedded Systems Security en el Visor de eventos. Para ello, realice las

siguientes acciones:

- En la lista **Componente**, seleccione el componente de Kaspersky Embedded Systems Security para el cual desea configurar el nivel de detalle.

  Para los componentes de Protección de archivos en tiempo real, Análisis a pedido y Actualización, se proporciona el registro de eventos mediante registros de tareas y el registro del evento. Para estos componentes, la tabla de lista de eventos contiene las columnas **Registro de tareas** y **Registro de Eventos de Windows**. Los eventos para los componentes Cuarentena y Copia de seguridad se registran en el registro de auditoría del sistema y el registro del evento. Para estos componentes, la tabla de lista de eventos contiene las columnas **Auditoría** y **Registro de Eventos de Windows**.

- En la lista **Nivel de importancia**, seleccione un nivel de detalle para los eventos en los registros de tarea, el registro de auditoría del sistema y el registro del evento para el componente seleccionado.

  En la siguiente tabla con una lista de eventos, las casillas están seleccionadas junto a los eventos que están registrados con registros de tarea, el registro de auditoría del sistema y el registro del evento, de acuerdo con el nivel de detalle actual.

- Si desea habilitar manualmente el registro de eventos específicos para un componente seleccionado, realice las siguientes acciones:

a. En la lista **Nivel de importancia**, seleccione **Personalizado**.

b. En la tabla con la lista de eventos, las casillas están seleccionadas junto a los eventos que desea que se registren en los registros de tarea, el registro de auditoría del sistema y el registro del evento.

- En la pestaña **Avanzado**, configure las opciones de almacenamiento de registros y umbrales de generación de eventos para el estado de protección del equipo:

  - En la sección **Almacenamiento de registros**:

    - **Carpeta de registros**

      Ruta de la carpeta del registro en formato UNC (Convención de nomenclatura universal).

      Ruta predeterminada: C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports\.

      Si se cambia la ruta predeterminada, se crea una carpeta con el nombre correspondiente. Los registros nuevos se almacenarán en la carpeta nueva. Los viejos registros se conservarán.

    - **Eliminar registros de tareas anteriores a (días)**

      La casilla habilita o deshabilita una función que elimina registros con los resultados de la ejecución de tareas finalizadas y eventos publicados en registros de tareas en ejecución luego del período especificado (valor predeterminado: 30 días).

      Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security elimina los registros con los resultados de la ejecución de tareas finalizadas y los eventos publicados en registros de tareas en ejecución luego del periodo especificado.

      De forma predeterminada, la casilla está activada.

    - **Eliminar del registro de auditoría del sistema los eventos anteriores a (días)**

      La casilla habilita o deshabilita una función que elimina eventos grabados en el registro

de auditoría del sistema luego del período especificado (valor predeterminado: 60 días).

Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security elimina los eventos grabados en el registro de auditoría del sistema luego del periodo especificado.

De forma predeterminada, la casilla está desactivada.

- En la sección **Umbrales de generación de eventos**:
  - Especifique el número de días después de los cuales se producirán los eventos *La base de datos de la aplicación está desactualizada*, *La base de datos de la aplicación es obsoleta* y *Hace mucho tiempo que no se realiza un análisis de áreas críticas*.

Tabla 36. Umbrales de generación de eventos

Configuración	Umbrales de generación de eventos.
Descripción	Puede especificar umbrales para generar los siguientes tipos de eventos: *La base de datos de la aplicación está desactualizada* y *La base de datos de la aplicación es obsoleta*. Este evento ocurre si la base de datos de Kaspersky Embedded Systems Security no se ha actualizado durante el periodo (en días) especificado por el parámetro desde la fecha de lanzamiento de las actualizaciones de la base de datos más recientemente instaladas. Puede configurar notificaciones de administrador para este evento. *Hace mucho tiempo que no se realiza un análisis de áreas críticas*. Este evento ocurre si no se realiza ninguna de las tareas marcadas con la casilla de verificación **Considerar la tarea como análisis de áreas críticas** durante el número de días especificado.
Valores posibles	Número de días de 1 a 365.
Valor predeterminado	Las bases de datos de la aplicación son obsoletas: 7 días; Las bases de datos de la aplicación son extremadamente obsoletas: 14 días; Hace mucho tiempo que no se realiza un análisis de áreas críticas: 30 días.

- En la pestaña **Integración de SIEM**, configure los ajustes para publicar eventos de auditoría y eventos de desempeño de la tarea en el servidor syslog (consulte la sección “Configuración de las opciones de la integración de SIEM”, en la página 208).

3. Haga clic en **Aceptar** para guardar los cambios.

En esta sección

Acerca de la integración de SIEM

Para reducir la carga en dispositivos de rendimiento reducido y reducir el riesgo de la degradación del sistema a consecuencia de volúmenes aumentados de registros de la aplicación, puede configurar la publicación de eventos de auditoría y eventos de rendimiento de la tarea en el *servidor syslog* mediante el protocolo Syslog.

Un servidor syslog es un servidor externo para agregar eventos (SIEM). Obtiene y analiza eventos recibidos y también realiza otras acciones para administrar registros.

Puede usar la integración de SIEM en dos modos:

- Duplicar eventos en el servidor syslog: este modo indica que todos los eventos de rendimiento de la tarea cuya publicación se configura en la configuración de registros, así como todos los eventos de auditoría del sistema, continúen almacenándose en el equipo local hasta después de que se envíen a SIEM.

  Se recomienda usar este modo para reducir máximamente la carga en el equipo protegido.

- Eliminar copias locales de eventos: este modo indica que todos los eventos que se registran durante el funcionamiento de la aplicación y se publican en SIEM se eliminen del equipo local.

  La aplicación nunca elimina las versiones locales del registro de seguridad.

Kaspersky Embedded Systems Security puede convertir eventos en los registros de la aplicación a formatos admitidos por el servidor syslog, de modo que dichos eventos se puedan transmitir y sean reconocidos de manera exitosa por SIEM. La aplicación admite la conversión al formato de datos estructurado y al formato JSON.

Se recomienda seleccionar el formato de eventos basados en la configuración del SIEM utilizado.

Configuraciones de confiabilidad

Para reducir el riesgo de retransmisiones no exitosas de eventos a SIEM, puede definir la configuración para realizar una conexión con el servidor syslog idéntico.

El servidor syslog idéntico es un servidor syslog adicional al cual la aplicación cambia automáticamente si la conexión con el servidor syslog principal no está disponible o si el servidor principal no se puede utilizar.

Kaspersky Embedded Systems Security también le notifica sobre intentos no exitosos de establecer una conexión con SIEM y sobre errores que envían los eventos a SIEM mediante los eventos de auditoría del sistema.

Configuración de las opciones de integración de SIEM

De forma predeterminada, la integración de SIEM no se usa. Puede habilitar y deshabilitar la integración de SIEM y configurar las opciones de funcionalidad (consulte la tabla a continuación).

Tabla 37. Configuración de integración de SIEM

Configuración	Valor predeterminado	Descripción
Enviar eventos a un servidor remoto de Syslog, mediante el protocolo de Syslog	No aplicado	Puede habilitar o deshabilitar la integración de SIEM al seleccionar o al desactivar la casilla, respectivamente.
Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog	No aplicado	Puede ajustar la configuración para almacenar copias locales de registros después de que se envíen a SIEM al seleccionar o al desactivar la casilla.
Formato de los eventos	Datos estructurados	Puede seleccionar uno de dos formatos a los cuales la aplicación convierte sus eventos antes de enviarlos al servidor syslog para el mejor reconocimiento de estos eventos por SIEM.
Protocolo de conexión	TCP	Puede usar la lista desplegable para configurar la conexión con los servidores syslog principal e idéntico mediante protocolos de TCP o UDP.

Configuración	Valor predeterminado	Descripción
Configuración de conexión al servidor syslog principal	Dirección IP: 127.0.0.1 Puerto: 514	Puede usar los campos apropiados para configurar la dirección IP y el puerto usados para conectarse al servidor syslog principal. Puede especificar la dirección IP solo en el formato IPv4.
Utilice el servidor reflejado de Syslog si no es posible acceder al servidor principal	No aplicado	Puede usar la casilla para habilitar o deshabilitar el uso de un servidor syslog idéntico.
Configuración de conexión al servidor syslog idéntico	Dirección IP: 127.0.0.1 Puerto: 514	Puede usar los campos apropiados para configurar la dirección IP y el puerto usados para conectarse al servidor reflejado de Syslog. Puede especificar la dirección IP solo en el formato IPv4.

► *Para configurar la integración de SIEM:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Registros y notificaciones**.
2. Seleccione **Propiedades**.

   Se abre la ventana **Configuración de registros y notificaciones**.
3. Seleccione la pestaña **Integración de SIEM**.
4. En la sección **Ajustes de integración**, seleccione la casilla **Enviar eventos a un servidor remoto de Syslog, mediante el protocolo de Syslog**.

   La casilla habilita o deshabilita la funcionalidad para enviar eventos publicados a un servidor syslog externo.

   Si la casilla se selecciona, la aplicación envía eventos publicados a SIEM según la configuración de integración de SIEM establecida.

   Si la casilla se desactiva, la aplicación no realiza la integración de SIEM. No puede ajustar la configuración de integración de SIEM si la casilla se desactiva.

   De forma predeterminada, la casilla está desactivada.
5. Si es necesario, en la sección **Ajustes de integración**, seleccione la casilla **Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog**.

   La casilla habilita o deshabilita la eliminación de copias locales de registros cuando se envían a SIEM.

   Si la casilla se selecciona, la aplicación elimina las copias locales de eventos después de que se han publicado correctamente en SIEM. Este modo se recomienda en equipos de rendimiento reducido.

   Si la casilla se desactiva, la aplicación solo envía eventos a SIEM. Las copias de los de registros continúan almacenándose a nivel local.

   De forma predeterminada, la casilla está desactivada.

El estado de la casilla **Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog** no afecta la configuración para almacenar eventos del registro de seguridad: la aplicación nunca elimina automáticamente eventos del registro de seguridad.

6. En la sección **Formato de los eventos**, especifique el formato al cual desea convertir los eventos operativos de la aplicación de modo que se puedan enviar a SIEM.

   De forma predeterminada, la aplicación los convierte en el formato de datos estructurado.

7. En la sección **Configuración de conexión**:

   - Especifique el protocolo de conexión de SIEM.
   - Especifique la configuración para conectarse al servidor syslog principal.

     Puede especificar una dirección IP en formato IPv4 únicamente.
   - Seleccione la casilla **Utilice el servidor reflejado de Syslog si no es posible acceder al servidor principal** si desea que la aplicación use otra configuración de conexión cuando sea incapaz de enviar eventos al servidor syslog principal.
     - Especifique la siguiente configuración para conectarse al servidor syslog idéntico: **Dirección IP** y **Puerto**.

       Los campos **Dirección IP** y **Puerto** para el servidor syslog idéntico no se pueden modificar si se desactiva la casilla **Utilice el servidor reflejado de Syslog si no es posible acceder al servidor principal**.

       Puede especificar una dirección IP en formato IPv4 únicamente.

8. Haga clic en **Aceptar**.

   La configuración de integración de SIEM establecida se aplicará.

Configuración de notificación

Esta sección brinda información sobre las formas en que los usuarios y los administradores de Kaspersky Embedded Systems Security pueden recibir notificaciones sobre eventos de la aplicación y el estado de protección del equipo, además de instrucciones sobre cómo configurar notificaciones.

En este capítulo

Métodos de notificación de administrador y usuario

Puede configurar la aplicación para que notifique al administrador y a los usuarios que tienen acceso al equipo protegido sobre eventos en el funcionamiento de Kaspersky Embedded Systems Security y el estado de la protección antivirus del equipo.

La aplicación garantiza el rendimiento de las tareas siguientes:

- El administrador puede recibir información sobre eventos de tipos seleccionados.
- Los usuarios de LAN que acceden a un equipo protegido y los usuarios de equipos de terminales pueden recibir información sobre eventos del tipo *Objeto detectado* en la tarea de Protección de archivos en tiempo real.

En la Consola de la aplicación, las notificaciones para administradores y usuarios se pueden activar mediante diversos métodos:

- Métodos de notificación para usuarios:
  a. Herramientas de servicio de terminales.

     Se puede aplicar este método para notificar a los usuarios de equipos terminales si el equipo protegido se utiliza como terminal.

  b. Herramientas de servicio de mensajes.

     Se puede aplicar este método para la notificación a través de los servicios de mensajes de Microsoft Windows.
- Métodos de notificación para el administrador:
  a. Herramientas de servicio de mensajes.

     Se puede aplicar este método para la notificación a través de los servicios de mensajes de Microsoft Windows.

  b. Ejecución de un archivo ejecutable.

     Este método ejecuta un archivo ejecutable almacenado en la unidad local del equipo protegido, cuando se produce el evento.

  c. Envío por correo electrónico.

     Este método utiliza el correo electrónico para transmitir los mensajes.

Puede crear un texto del mensaje para tipos de eventos individuales. Puede incluir un campo de información para describir un evento. De manera predeterminada, la aplicación utiliza un texto predefinido para notificar a los usuarios.

Configuración de notificaciones de administrador y usuario

La configuración de notificaciones de eventos ofrece diversos métodos para configurar y redactar un texto del mensaje.

► *Para configurar los valores de notificaciones de eventos, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Registros y notificaciones** y seleccione **Propiedades**.

   Se abre la ventana **Configuración de registros y notificaciones**.
2. En la pestaña **Notificaciones**, seleccione el modo de notificación:
   a. Seleccione el evento para el que desea seleccionar un método de notificación de la lista **Tipo de evento**.
   b. En el grupo de configuraciones **Notificar a los administradores** o **Notificar a los usuarios**,

seleccione la casilla de verificación junto a los métodos de notificación que desea configurar.

> Puede configurar las notificaciones del usuario solo para el evento **Objeto detectado**, el evento **Almacenamiento masivo dudoso detectado y restringido** y el evento **El host está en la lista de dudosos**.

3. Para agregar el texto de un mensaje:
   a. Haga clic en el botón **Texto del mensaje**.
   b. En la ventana que se abre, introduzca el texto que se mostrará en el mensaje del evento correspondiente.

> Se puede crear un texto del mensaje para varios tipos de eventos: después de haber seleccionado un método de notificación para un tipo de evento, seleccione los otros tipos de eventos para los que desea utilizar el mismo texto del mensaje mediante las teclas **Ctrl** o **Mayús** y, luego, haga clic en el botón **Texto del mensaje**.

   c. Para agregar campos con información sobre un evento, haga clic en el botón **Macro** y seleccione los campos relevantes de la lista desplegable. En la tabla de esta sección se describen campos con información sobre los eventos.
   d. Para restaurar el texto del mensaje del evento predeterminado, haga clic en el botón **Predeterminado**.
4. Para configurar los métodos seleccionados de notificación del administrador sobre el evento seleccionado, seleccione la pestaña **Notificaciones**, haga clic en el botón **Configurar** en la sección **Notificar a los administradores** y configure los métodos seleccionados en la ventana **Configuración avanzada**. Para ello, realice las siguientes acciones:
   a. Para las notificaciones por correo electrónico, abra la pestaña **Correo electrónico** y especifique las direcciones de correo electrónico de los destinatarios (delimite las direcciones con punto y coma), el nombre o la dirección de red del servidor SMTP y el número de puerto en los campos correspondientes. Si es necesario, especifique el texto que se mostrará en los campos **Asunto** y **De**. El texto del campo **Asunto** también puede incluir variables con información sobre el evento (consulte la tabla a continuación).

      Si desea aplicar la autenticación con cuentas de usuario al establecer conexión con el servidor SMTP, seleccione **Usar autenticación SMTP** en el grupo **Configuración de autenticación** y especifique el nombre y la contraseña del usuario cuya cuenta de usuario se autenticará.
   b. Para notificaciones con el **Servicio Windows Messenger**, cree una lista de equipos de destinatarios para notificaciones en la pestaña **Servicio Windows Messenger**: para cada equipo que desea agregar, presione el botón **Agregar** y escriba su nombre de red en el campo de entrada.
   c. Para ejecutar un archivo ejecutable, seleccione el archivo en una unidad local del equipo protegido que se ejecutará en el equipo activado por el evento o introduzca la ruta completa a él en la pestaña **Archivo ejecutable**. Introduzca el nombre de usuario y la contraseña que se utilizarán para ejecutar el archivo.

      Se pueden utilizar variables del entorno del sistema cuando se especifica la ruta al archivo ejecutable; no se permiten variables del entorno del usuario.

      Si desea limitar la cantidad de mensajes para un tipo de evento durante un periodo, en la pestaña **Avanzado** seleccione **No enviar la misma notificación más de** y especifique la cantidad de veces y la unidad de tiempo.

5. Haga clic en **Aceptar**.

La configuración de notificaciones se guarda.

Tabla 38. Campos con información sobre el evento

Variable	Descripción
%EVENT_TYPE%	Tipo de evento.
%EVENT_TIME%	Hora del evento.
%EVENT_SEVERITY%	Nivel de importancia.
%OBJECT%	Nombre del objeto (en tareas de Protección del equipo en tiempo real y de Análisis a pedido). La tarea de Actualización de módulos del programa incluye el nombre de la actualización y la dirección de la página web con información sobre la actualización.
%VIRUS_NAME%	El nombre del objeto según la clasificación de la Enciclopedia de Virus https://encyclopedia.kaspersky.com/knowledge/classification/. Este nombre se incluye en el nombre completo del objeto detectado en los resultados de detección de objetos de Kaspersky Embedded Systems Security. Puede ver el nombre completo del objeto detectado en el registro de tareas (consulte la sección “Visualización de estadísticas e información sobre una tarea de Kaspersky Embedded Systems Security en registros de tareas” en la página 202).
%VIRUS_TYPE%	El tipo de objeto detectado según la clasificación de Kaspersky Lab, como “virus” o “troyano”. Se incluye en el nombre completo del objeto detectado, que devuelve Kaspersky Embedded Systems Security cuando detecta un objeto infectado o probablemente infectado. Puede ver el nombre completo del objeto detectado en el registro de tareas.
%USER_COMPUTER%	En la tarea de Protección de archivos en tiempo real, el nombre del equipo para el usuario que accedió al objeto en el equipo.
%USER_NAME%	En la tarea de Protección de archivos en tiempo real, el nombre del usuario que accedió al objeto en el equipo.
%FROM_COMPUTER%	Nombre del equipo protegido en el que se originó la notificación.
%EVENT_REASON%	Motivo por el cual ocurrió el evento (algunos eventos no tienen este campo).
%ERROR_CODE%	Código de error (utilizado solo para evento de "error de tarea interno").
%TASK_NAME%	Nombre de la tarea (solo para eventos relacionados con el rendimiento de la tarea).

Cómo iniciar y detener Kaspersky Embedded Systems Security

Esta sección contiene información sobre el inicio de la Consola de la aplicación y sobre el inicio y la detención de servicio de Kaspersky Security.

En este capítulo

Inicio del Complemento de administración de Kaspersky Embedded Systems Security

No se requiere ninguna acción avanzada para iniciar el Complemento de administración de Kaspersky Embedded Systems Security en Kaspersky Security Center. Después de que el complemento se instala en el equipo del administrador, se inicia simultáneamente con Kaspersky Security Center. La información detallada sobre Kaspersky Security Center inicial se puede encontrar en la *Ayuda de Kaspersky Security Center*.

Inicio de la Consola de Kaspersky Embedded Systems Security desde el menú Inicio

Los nombres de configuración pueden variar en los diferentes sistemas operativos Windows.

► *Para iniciar la Consola de la aplicación desde el menú **Inicio**:*

1. En el menú **Inicio**, seleccione **Programas** > **Kaspersky Embedded Systems Security** > **Herramientas de administración** > **Consola de Kaspersky Embedded Systems Security**.

Para agregar otros complementos a la Consola de la aplicación, abra la Consola en modo de creación.

► *Para iniciar la Consola de la aplicación en modo de creación, siga estos pasos:*

1. En el menú **Iniciar**, seleccione **Programas** > **Kaspersky Embedded Systems Security** > **Herramientas de administración**.
2. En el menú contextual de la Consola de la aplicación, seleccione el comando **Creación**.

Se inicia la Consola de la aplicación en modo de creación.

Si la Consola de la aplicación se ha iniciado en el equipo protegido, se abrirá la ventana Consola de la aplicación.

Si inició la Consola de la aplicación en otro equipo que no es el protegido, conéctese con el equipo protegido.

► *Para conectarse con un equipo protegido:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security**.
2. Seleccione el comando **Conectarse a otro equipo**.

   Se abre la ventana **Seleccionar equipo**.
3. Seleccione **Otro equipo** en la ventana que se abre.
4. Especifique el nombre de la red del equipo protegido en el campo de entrada a la derecha.
5. Haga clic en **Aceptar**.

La Consola de la aplicación se conectará con un equipo protegido.

Si la cuenta del usuario que usa para iniciar sesión en Microsoft Windows no tiene permisos suficientes para acceder al servicio de Kaspersky Security Management en el equipo, seleccione la casilla de verificación **Conectarse como usuario** y especifique una cuenta de usuario diferente que tenga tales permisos.

Inicio y detención del servicio de Kaspersky Security

De forma predeterminada, el servicio de Kaspersky Security se inicia automáticamente después del inicio del sistema operativo. El servicio de Kaspersky Security administra procesos de trabajo en los que se ejecutan tareas de actualización, Protección del equipo en tiempo real, Control del equipo y Análisis a pedido.

De forma predeterminada, cuando se inicia el servicio de Kaspersky Embedded Systems Security, se inician las tareas de Protección de archivos en tiempo real, Análisis al inicio del sistema operativo y Control de integridad de la aplicación, así como otras tareas que están programadas para iniciarse **Al inicio de la aplicación**.

Si se detiene el servicio de Kaspersky Security, todas las tareas en ejecución se detienen. Después de reiniciar el servicio de Kaspersky Security, la aplicación inicia automáticamente solo aquellas tareas cuya programación tiene la frecuencia de inicio configurada en **Al inicio de la aplicación**, mientras que las otras tareas se deben iniciar manualmente.

Puede iniciar y detener el servicio de Kaspersky Security con el menú contextual del nodo **Kaspersky Embedded Systems Security** o con el complemento Servicios de Microsoft Windows.

Puede iniciar y detener Kaspersky Embedded Systems Security si es miembro del grupo de Administradores en el equipo protegido.

► *Para detener o iniciar la aplicación con la Consola de la aplicación, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security**.
2. Seleccione uno de los siguientes elementos:
   - **Detener el servicio**.
   - **Iniciar el servicio**.

El servicio de Kaspersky Security se iniciará o se detendrá.

Inicio de los componentes de Kaspersky Embedded Systems Security en el modo seguro del sistema operativo

Esta sección proporciona información sobre cómo funciona Kaspersky Embedded Systems Security en el modo seguro del sistema operativo.

En este capítulo

Acerca de Kaspersky Embedded Systems Security cuando se ejecuta en el modo seguro del sistema operativo

Los componentes de Kaspersky Embedded Systems Security pueden iniciarse al cargar el sistema operativo en modo seguro. Además de Kaspersky Security Service (kavfs.exe), se carga el controlador klam.sys, que se utiliza para registrar el servicio de Kaspersky Security como un servicio protegido durante el inicio del sistema operativo. Para obtener más información, consulte la sección Registro del servicio de Kaspersky Security como servicio protegido.

Kaspersky Embedded Systems Security puede iniciarse en los siguientes modos seguros del sistema operativo:

- Modo seguro mínimo: este modo se inicia cuando se selecciona la opción estándar del modo seguro del sistema operativo. En ese momento, Kaspersky Embedded Systems Security puede iniciar los siguientes componentes:
  - Protección de archivos en tiempo real.
  - Análisis a pedido.
  - Control de inicio de aplicaciones y Generador de reglas para Control de inicio de aplicaciones.
  - Inspección de registros.
  - Monitor de integridad de archivos.
  - Control de integridad de la aplicación.

- Modo seguro con red: este modo se inicia cuando el sistema operativo se carga en modo seguro con controladores de red. Además de los componentes que se inician en el modo seguro mínimo, Kaspersky Embedded Systems Security puede iniciar los siguientes componentes:
  - Actualización de bases de datos
  - Actualización de módulos del programa

Inicio de Kaspersky Embedded Systems Security en modo seguro

De forma predeterminada, Kaspersky Embedded Systems Security no se inicia al cargar el sistema operativo en modo seguro.

► *Para hacer que Kaspersky Embedded Systems Security se inicie en el modo seguro del sistema operativo, realice las siguientes acciones:*

1. Inicie el editor de registro de Windows (C:\Windows\regedit.exe).
2. Abra la clave [HKEY_LOCAL_MACHINE \ SYSTEM\CurrentControlSet\Services\klam\Parameters] del registro del sistema.
3. Abra el parámetro LoadInSafeMode.
4. Establezca el valor `1`.
5. Haga clic en **Aceptar**.

► *Para cancelar el inicio de Kaspersky Embedded Systems Security en el modo seguro del sistema operativo, realice las siguientes acciones:*

1. Inicie el editor de registro de Windows (C:\Windows\regedit.exe).
2. Abra la clave [HKEY_LOCAL_MACHINE \ SYSTEM\CurrentControlSet\Services\klam\Parameters] del registro del sistema.
3. Abra el parámetro LoadInSafeMode.
4. Establezca el valor `0`.
5. Haga clic en **Aceptar**.

Autoprotección de Kaspersky Embedded Systems Security

Esta sección brinda información sobre los mecanismos de autoprotección de Kaspersky Embedded Systems Security.

En este capítulo

Acerca de la autoprotección de Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security incluye mecanismos de autoprotección que protegen la aplicación contra la modificación o eliminación de sus carpetas en el disco duro, los procesos de memoria y las entradas de registro del sistema.

Protección contra cambios de carpetas con componentes de Kaspersky Embedded Systems Security instalados

Kaspersky Embedded Systems Security restringe el cambio de nombre y la eliminación de carpetas con los componentes de la aplicación instalada para cualquier cuenta de usuario. De forma predeterminada, las rutas de las carpetas de instalación de la aplicación son las siguientes:

- En la versión de 32 bits de Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- En la versión de 64 bits de Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

Protección contra cambios en las claves de registro de Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security restringe los derechos de acceso a las siguientes ramas y claves del registro, que proporcionan la carga de los controladores y servicios de la aplicación:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\CrashDump] (en la versión de 64 bits de Microsoft Windows)
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\Trace]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Trace] (en la versión de 64 bits de Microsoft Windows)

Los derechos para cambiar estas ramas y claves del registro se otorgan solo a la cuenta del Sistema Local (SISTEMA) . Las cuentas de usuario y administrador se otorgan con derechos de solo lectura.

Registro del servicio de Kaspersky Security como servicio protegido

La tecnología *Luz de proceso protegido* (también denominada “PPL”) garantiza que el sistema operativo solo cargue servicios y procesos de confianza. Para que un servicio se ejecute como servicio protegido, debe instalarse un controlador de *antimalware de ejecución temprana* en el equipo protegido.

Un controlador de *antimalware de ejecución temprana* (también denominado “ELAM”) ofrece protección para los equipos en la red cuando se inician, antes de que se inicien los controladores de terceros.

El controlador ELAM se instala durante la instalación de Kaspersky Embedded Systems Security, y se utiliza para registrar el servicio de Kaspersky Security como PPL cuando se inicia el sistema operativo. Cuando el servicio de Kaspersky Security (KAVFS) se inicia como proceso protegido del sistema, otros procesos no protegidos en el sistema no pueden inyectar subprocesos, escribir en la memoria virtual del proceso protegido o detener el servicio.

Cuando un proceso se inicia como PPL, no puede ser administrado por un usuario ignorando los permisos del usuario asignados. El registro del servicio de Kaspersky Security como PPL usando el controlador ELAM se admite en sistemas operativos Microsoft Windows 10 y superiores. Si instala Kaspersky Embedded Systems Security en un servidor que ejecuta un sistema operativo compatible con PPL, no estará disponible la administración de permisos para el servicio de Kaspersky Security (KAVFS).

► *Para instalar Kaspersky Embedded Systems Security como PPL, ejecute el siguiente comando:*

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Administración de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security

Esta sección contiene información acerca de los permisos para administrar Kaspersky Embedded Systems Security y los servicios de Windows registrados por la aplicación, e instrucciones sobre cómo configurar estos permisos.

En este capítulo

Acerca de los permisos para administrar Kaspersky Embedded Systems Security

De forma predeterminada, el acceso a todas las funciones de Kaspersky Embedded Systems Security se concede a usuarios del grupo de Administradores en el equipo protegido, los usuarios del grupo de Administradores ESS creado en el equipo protegido durante la instalación de Kaspersky Embedded Systems Security y al grupo SYSTEM.

Los usuarios que tienen el acceso a la función **Editar** permisos de Kaspersky Embedded Systems Security pueden conceder acceso a las funciones de Kaspersky Embedded Systems Security a otros usuarios registrados en el equipo protegido o incluidos en el dominio.

Los usuarios que no están registrados en la lista de usuarios de Kaspersky Embedded Systems Security no pueden abrir la Consola de la aplicación.

Puede elegir uno de los siguientes niveles preestablecidos de acceso para un usuario o un grupo de usuarios:

- **Control total**: acceso a todas las funciones de la aplicación, p. ej., la capacidad de ver y modificar la configuración general de Kaspersky Embedded Systems Security, la configuración de los componentes y los permisos de usuarios de Kaspersky Embedded Systems Security, y la capacidad de ver estadísticas de Kaspersky Embedded Systems Security.
- **Editar**: acceso a todas las funciones de la aplicación, excepto la edición de permisos del usuario, p. ej., la capacidad de ver y editar la configuración general de Kaspersky Embedded Systems Security y los parámetros de los componentes de Kaspersky Embedded Systems Security.
- **Lectura**: la capacidad de ver la configuración general de Kaspersky Embedded Systems Security, la configuración de los componentes de Kaspersky Embedded Systems Security, las estadísticas de Kaspersky Embedded Systems Security y los permisos de usuario de Kaspersky Embedded Systems Security.

También puede configurar permisos de acceso avanzados: permita o bloquee el acceso a funciones específicas de Kaspersky Embedded Systems Security.

Si ha configurado manualmente permisos de acceso para un usuario o grupo, el nivel de acceso **Permisos especiales** se configura para este usuario o grupo.

Tabla 39. Acerca de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security

Derechos del usuario	Descripción
Administración de tareas	Capacidad para iniciar/detener/pausar/reanudar tareas de Kaspersky Embedded Systems Security.
Crear y eliminar tareas de Análisis a pedido	Capacidad para crear y eliminar tareas de Análisis a pedido.
Editar la configuración	Capacidad para: • Importar ajustes de Kaspersky Embedded Systems Security desde un archivo de configuración. • Editar la configuración de la aplicación.
Leer configuración	Capacidad para: • Ver la configuración general y la configuración de tareas de Kaspersky Embedded Systems Security. • Exportar la configuración de Kaspersky Embedded Systems Security a un archivo de configuración. • Ver la configuración de los registros de tareas, del registro de auditoría del sistema y de las notificaciones.
Administrar repositorios	Capacidad para: • Mover objetos a Cuarentena. • Eliminar objetos de la Cuarentena y de la Copia de seguridad. • Restaurar objetos de la Cuarentena y de la Copia de seguridad.
Administrar registros	Capacidad para eliminar registros de tareas y borrar el registro de auditoría del sistema.
Leer registros	Capacidad para ver eventos del antivirus en los registros de tareas y el registro de auditoría del sistema.

Derechos del usuario	Descripción
Leer estadísticas	Capacidad para ver estadísticas por cada tarea de Kaspersky Embedded Systems Security.
Licencia de la aplicación	Capacidad de activar Kaspersky Embedded Systems Security.
Desinstalar la aplicación	Capacidad de desinstalar Kaspersky Embedded Systems Security.
Leer permisos	Capacidad para ver la lista de usuarios de Kaspersky Embedded Systems Security y los privilegios de acceso de los usuarios.
Editar permisos	Capacidad para: • Modificar la lista de usuarios con acceso a la administración de la aplicación. • Modificar los permisos de acceso para las funciones de Kaspersky Embedded Systems Security.

Acerca de los permisos para administrar servicios registrados

Durante la instalación, Kaspersky Embedded Systems Security registra en Windows el servicio de Kaspersky Security (KAVFS), el servicio de Kaspersky Security Management (KAVFSGT) y la Prevención de exploits de Kaspersky Security (KAVFSSLP).

El registro de Kaspersky Security Service como Protected Process Light mediante el controlador ELAM se admite en sistemas operativos Microsoft Windows 10 y superiores. Cuando un proceso se inicia como PPL, no puede ser administrado por un usuario ignorando los permisos del usuario asignados. Si instala Kaspersky Embedded Systems Security en un equipo que ejecuta un sistema operativo compatible con PPL, no estará disponible la administración de permisos para el servicio de Kaspersky Security (KAVFS).

Servicio de Kaspersky Security

De forma predeterminada, los permisos de acceso para administrar el servicio de Kaspersky Security se conceden a los usuarios del grupo Administradores en el equipo protegido, así como a los grupos de SERVICE e INTERACTIVE con permisos de lectura y al grupo SYSTEM con permisos de lectura y ejecución.

Los usuarios que tienen acceso a funciones del nivel Editar permisos (consulte la sección “Acceso protegido por contraseña a funciones de Kaspersky Embedded Systems Security” en la página 227) puede otorgar permisos de acceso para administrar el servicio de Kaspersky Security a los demás usuarios registrados en el equipo protegido o incluido en el dominio.

Servicio de Kaspersky Security Management

Para administrar la aplicación mediante la Consola de la aplicación instalada en otro equipo, la cuenta con los permisos para conectarse a Kaspersky Embedded Systems Security debe tener acceso absoluto al servicio de Kaspersky Security Management en el equipo protegido.

De forma predeterminada, se les concede acceso al servicio de Kaspersky Security Management a los usuarios del grupo de administración del equipo protegido y a los usuarios del grupo de administración de ESS que se haya creado en el equipo protegido durante la instalación de Kaspersky Embedded Systems Security.

Solo puede administrar el servicio de Kaspersky Security Management a través del complemento Servicios de Microsoft Windows.

Prevención de exploits de Kaspersky Security

De forma predeterminada, los permisos de acceso para administrar el servicio de Kaspersky Security Exploit Prevention se conceden a los usuarios del grupo Administradores en el equipo protegido, así como al grupo SYSTEM con permisos de lectura y ejecución.

Acerca de los permisos para administrar el servicio de Kaspersky Security

Durante la instalación, Kaspersky Embedded Systems Security registra el servicio de Kaspersky Security (KAVFS) en Windows, e internamente habilita los componentes funcionales que se comienzan cuando se inicia el sistema operativo. Para reducir el riesgo de que un tercero acceda a las funciones de la aplicación y la configuración de seguridad en un equipo protegido a través de la administración del servicio de Kaspersky Security, puede restringir los permisos de administración del servicio de Kaspersky Security desde la Consola de la aplicación o el Complemento de administración.

De forma predeterminada, los permisos de acceso para administrar el servicio de Kaspersky Security se conceden a usuarios en el grupo de Administradores en el equipo protegido. Los permisos de lectura se conceden a los grupos de SERVICIO e INTERACTIVOS, y los permisos de lectura y ejecución se conceden al grupo SYSTEM.

No se puede eliminar la cuenta de usuario de SYSTEM o modifica permisos para esta cuenta. Si se modifican los permisos de la cuenta SYSTEM, los privilegios máximos se restauran para esta cuenta cuando guarda los cambios.

Los usuarios que tienen acceso a funciones (consulte la sección “Acerca de los permisos para administrar Kaspersky Embedded Systems Security” en la página 220) que requieren permisos de Edición pueden otorgar permisos de acceso para administrar el servicio de Kaspersky Security a otros usuarios registrados en el equipo protegido o incluido en el dominio.

Puede elegir uno de los siguientes niveles predeterminados de permisos para un usuario o grupo de usuarios de Kaspersky Embedded Systems Security para administrar el servicio de Kaspersky Security:

- **Control total**: capacidad de ver y modificar la configuración general y los permisos de usuario para el servicio de Kaspersky Security, e iniciar y detener el servicio de Kaspersky Security.
- **Lectura**: capacidad de ver la configuración general y los permisos de usuario del servicio de Kaspersky Security.
- **Modificación**: capacidad de ver y modificar la configuración general y los permisos de usuario del servicio de Kaspersky Security.
- **Ejecución**: capacidad de iniciar y detener el servicio de Kaspersky Security.

También puede configurar los permisos del acceso avanzado: autorice o deniegue el acceso a funciones específicas de Kaspersky Embedded Systems Security (ver la tabla a continuación).

Si ha configurado manualmente permisos de acceso para un usuario o grupo, el nivel de acceso **Permisos especiales** se configura para este usuario o grupo.

Tabla 40. Permisos de acceso para las funciones del servicio de Kaspersky Security.

Función	Descripción
Ver configuraciones del servicio	Capacidad para ver las configuraciones generales y los permisos de usuario del servicio de Kaspersky Security.
Solicitar estado del servicio al Administrador de control de servicios	Capacidad para solicitar el estado de ejecución del servicio de Kaspersky Security desde el Administrador de control de servicios de Microsoft Windows.
Solicitar estado al servicio	Capacidad para solicitar el estado de ejecución del servicio desde el servicio de Kaspersky Security.
Leer lista de servicios dependientes	Capacidad para ver una lista de servicios de los que depende el servicio de Kaspersky Security y que dependen del servicio de Kaspersky Security.
Modificación de la configuración del servicio	Capacidad de ver y modificar la configuración general y los permisos del usuario del servicio de Kaspersky Security.
Iniciar el servicio	Capacidad para iniciar el servicio de Kaspersky Security.
Detener el servicio	Capacidad para detener el servicio de Kaspersky Security.
Pausar/reanudar el servicio	Capacidad para pausar y reanudar el servicio de Kaspersky Security.
Leer permisos	Capacidad para ver la lista de usuarios del servicio de Kaspersky Security y los privilegios de acceso de cada usuario.
Editar permisos	Capacidad para: • Agregar y eliminar usuarios del servicio de Kaspersky Security • Modificar los permisos de acceso de usuarios para el servicio de Kaspersky Security.
Eliminar el servicio	Capacidad para eliminar el registro del servicio de Kaspersky Security en el Administrador de control de servicios de Microsoft Windows.
Solicitudes definidas por el usuario al servicio	Capacidad para crear y enviar solicitudes de usuario al servicio de Kaspersky Security.

Acerca de los permisos de acceso para el servicio de Kaspersky Security Management

Puede revisar la lista de servicios de Kaspersky Embedded Systems Security.

Durante la instalación, Kaspersky Embedded Systems Security registra el servicio de Kaspersky Security Management (KAVFSGT). Para administrar la aplicación mediante la Consola de la aplicación instalada en otro equipo, la cuenta utilizada para conectarse a Kaspersky Embedded Systems Security debe tener acceso absoluto al servicio de Kaspersky Security Management en el equipo protegido.

De forma predeterminada, se les concede acceso al servicio de Kaspersky Security Management a los usuarios del grupo de administración del equipo protegido y a los usuarios del grupo de administración de ESS que se haya creado en el equipo protegido durante la instalación de Kaspersky Embedded Systems Security.

Puede administrar el servicio de Kaspersky Security Management solo a través del complemento Servicios de Microsoft Windows.

No puede autorizar o bloquear el acceso de los usuarios al servicio de Kaspersky Security Management con Kaspersky Embedded Systems Security.

Puede conectarse a Kaspersky Embedded Systems Security desde una cuenta local si se registró una cuenta con el mismo nombre de usuario y contraseña en el equipo protegido.

Configuración de los permisos de acceso para administrar Kaspersky Embedded Systems Security y el servicio de Kaspersky Security

Puede editar la lista de usuarios y grupos de usuarios autorizados para acceder a las funciones de Kaspersky Embedded Systems Security y administrar el servicio de Kaspersky Security. También puede editar los permisos de acceso de esos usuarios y grupos de usuarios.

► *Para agregar o quitar un usuario o un grupo de la lista:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.
4. En la sección **Adicional**, siga uno de estos pasos:
   - Haga clic en **Configurar** en la subsección **Permisos de acceso de usuario para administrar la aplicación** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar Kaspersky Embedded Systems Security.
   - Haga clic en **Configurar** en la subsección **Permisos del acceso del usuario para la administración del servicio de Kaspersky Security** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar el servicio de Kaspersky Security.

     Se abre la ventana del grupo **Permisos para Kaspersky Embedded Systems Security**.
5. En la ventana que se abre, realice las siguientes operaciones:
   - Para agregar un usuario o un grupo a la lista, haga clic en el botón **Agregar** y seleccione el usuario o

el grupo a quien desea otorgar privilegios.

- Para eliminar un usuario o un grupo de la lista, seleccione el usuario o el grupo cuyo acceso desea restringir, y haga clic en el botón **Eliminar**.

6. Haga clic en el botón **Aplicar**.

Los usuarios seleccionados (grupos) se agregan o se eliminan.

► *Para modificar permisos de un usuario o un grupo para la administración de Kaspersky Embedded Systems Security o el servicio de Kaspersky Security:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas" en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center" en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.

4. En la sección **Adicional**, siga uno de estos pasos:
   - Haga clic en **Configurar** en la subsección **Modificar los derechos de usuario para administrar la aplicación** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar Kaspersky Embedded Systems Security.
   - Haga clic en **Configurar** en la subsección **Modificar los derechos de usuario para administrar servicio de Kaspersky Security** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar la aplicación mediante el servicio de Kaspersky Security.

     Se abre la ventana del grupo **Permisos para Kaspersky Embedded Systems Security**.
5. En la ventana que se abre, en la lista **Nombres de usuarios o grupos**, seleccione el usuario o grupo de usuarios a los que desea cambiar los permisos.
6. En la sección **Permisos para <Usuario (Grupo)>**, seleccione las casillas de verificación **Autorizar** o **Denegar** para los siguientes niveles de acceso:
   - **Control total**: conjunto completo de permisos para administrar Kaspersky Embedded Systems Security o el servicio de Kaspersky Security.
   - **Lectura**:
     - Los permisos siguientes para administrar Kaspersky Embedded Systems Security: **Leer estadísticas**, **Leer configuración**, **Leer registros** y **Leer permisos**.
     - Los siguientes permisos para administrar el servicio de Kaspersky Security: **Leer configuración del servicio**, **Solicitar estado del servicio al Administrador de control de servicios**, **Solicitar**

estado al servicio, **Leer lista de servicios dependientes**, **Leer permisos**.

- **Modificación**:
  - Todos los permisos para administrar Kaspersky Embedded Systems Security, excepto **Editar permisos**
  - Los siguientes permisos para administrar el servicio de Kaspersky Security: **Modificar configuración del servicio**, **Leer permisos**.
- **Permisos especiales**: los siguientes permisos para administrar el servicio de Kaspersky Security: **Iniciar el servicio**, **Detener el servicio**, **Pausar o reanudar el servicio**, **Leer permisos**, **Solicitudes definidas por el usuario al servicio**.

7. Para establecer permisos avanzados para un usuario o grupo (**Permisos especiales**), haga clic en el botón **Avanzado**.
   a. En la ventana **Configuración de la seguridad avanzada para Kaspersky Embedded Systems Security** que se abre, seleccione el usuario o el grupo deseado.
   b. Haga clic en el botón **Editar**.
   c. En la lista desplegable ubicada en la parte superior de la ventana, seleccione el tipo de control de acceso (**Autorizar** o **Bloquear**).
   d. Seleccione las casillas de verificación al lado de las funciones que desea autorizar o bloquear para el usuario o el grupo seleccionado.
   e. Haga clic en **Aceptar**.
   f. En la ventana **Configuración de seguridad avanzada para Kaspersky Embedded Systems Security**, haga clic en **Aceptar**.
8. En la ventana de grupo **Permisos para Kaspersky Embedded Systems Security**, haga clic en el botón **Aplicar**.
9. Los permisos configurados para administrar Kaspersky Embedded Systems Security o el servicio de Kaspersky Security se guardarán.

Acceso protegido por contraseña a funciones de Kaspersky Embedded Systems Security

Puede restringir el acceso a la administración de la aplicación y a los servicios registrados mediante la configuración de permisos del usuario (consulte la sección "Administración de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security" en la página 220). También puede establecer la protección con contraseña en Kaspersky Embedded Systems Security para una protección adicional. La protección con contraseña permite establecer un límite adicional para la administración y la ejecución de los comandos de la línea de comandos de la Consola de la aplicación. Si se aplicó la protección con contraseña, Kaspersky Embedded Systems Security requiere que todos los usuarios introduzcan la contraseña al iniciar la Consola de la aplicación o ejecutar comandos de la línea de comandos.

► *Para proteger el acceso a funciones de Kaspersky Embedded Systems Security:*

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security** y realice una de las siguientes acciones:
   - Haga clic en el vínculo **Propiedades de la aplicación** en el panel de detalles del nodo.
   - Seleccione **Propiedades** en el menú contextual del nodo.

Se abrirá la ventana **Configuración de la aplicación**.

2. En la pestaña **Seguridad y fiabilidad**, en **Ajustes de protección mediante contraseña**, haga clic en la casilla de verificación **Aplicar protección con contraseña**.

   Los campos **Contraseña** y **Confirmar contraseña** se activan.

3. En el campo **Contraseña**, escriba el valor que desea usar para proteger el acceso a las funciones de Kaspersky Embedded Systems Security.
4. En el campo **Confirmar contraseña**, escriba su contraseña nuevamente.
5. Haga clic en **Aceptar**.

Esta contraseña no se puede recuperar. Si pierde su contraseña pierde completamente el control de la aplicación. Además, será imposible desinstalar la aplicación del equipo protegido.

Puede reiniciar la contraseña en cualquier momento. Para hacerlo, desactive la casilla **Aplicar protección con contraseña** y guarde los cambios. Se deshabilitará la protección con contraseña y se eliminará la suma de control de la contraseña anterior. Ingrese una contraseña nueva.

Configuración de permisos de acceso en Kaspersky Security Center

Puede configurar permisos de acceso para administrar la aplicación y el servicio de Kaspersky Security en Kaspersky Security Center para un grupo de equipos o para un equipo independiente.

► *Para acceder a permisos para administrar la aplicación y el servicio de Kaspersky Security:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.
4. Abra la sección **Adicional** y realice lo siguiente:
   - Para configurar permisos de acceso para administrar Kaspersky Embedded Systems Security para un usuario o un grupo de usuarios, en la sección **Permisos de acceso de usuario para administrar la aplicación**, haga clic en el botón **Configurar**.
   - Para configurar permisos de acceso para administrar el servicio de Kaspersky Security para un

usuario o un grupo de usuarios, en la sección **Permisos de acceso para administrar el servicio de Kaspersky Security**, haga clic en el botón **Configurar**.

5. En la ventana que se abre, configure los privilegios de acceso (consulte la sección “Administración de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security” en la página 220) según sus necesidades.

Se guarda la configuración especificada.

Protección de archivos en tiempo real

Esta sección contiene información acerca de la tarea de Protección de archivos en tiempo real y cómo configurarla.

En este capítulo

Acerca de la tarea Protección de archivos en tiempo real

Cuando se está ejecutando la tarea de Protección de archivos en tiempo real, Kaspersky Embedded Systems Security analiza los siguientes objetos del equipo protegido cuando se accede a ellos:

- Archivos.
- Flujos de sistemas de archivos alternativos (flujos NTFS).
- Sectores de inicio y registros de inicio maestro en los discos duros locales y dispositivos externos.

Cuando una aplicación escribe un archivo en un equipo o lee un archivo desde él, Kaspersky Embedded Systems Security intercepta dicho archivo, lo analiza en busca de amenazas y, si detecta una amenaza, realiza una acción predeterminada o una acción que usted haya especificado: intenta desinfectar el archivo, lo pasa a Cuarentena o simplemente lo elimina si no se puede desinfectar. Antes de la desinfección o eliminación, Kaspersky Embedded Systems Security guarda una copia cifrada del archivo de origen en la carpeta de copia de seguridad. Kaspersky Embedded Systems Security restaura el archivo de cuarentena en la carpeta original si se ha desinfectado con éxito.

Kaspersky Embedded Systems Security también detecta malware para procesos que se ejecutan bajo el Subsistema de Windows para Linux®. Para tales procesos, la tarea de Protección de archivos en tiempo real aplica la acción definida por la configuración actual.

Acerca del alcance de la protección de la tarea y la configuración de seguridad

De forma predeterminada, la tarea de Protección de archivos en tiempo real protege a todos los objetos del sistema de archivos del equipo. Si no hay requisitos de seguridad para proteger todos los objetos del sistema de archivos o si desea excluir cualquier objeto del alcance de la tarea, puede limitar el alcance de la protección.

En la Consola de la aplicación, el alcance de la protección se muestra como un árbol o en la lista de recursos de archivos del equipo que Kaspersky Embedded Systems Security puede controlar. De forma predeterminada, los recursos de archivos en red del equipo protegido se muestran en un modo de vista de lista.

En el Complemento de administración, solo está disponible la vista de la lista.

► *Para ver recursos de archivos en red en el modo de vista de árbol en la Consola de la aplicación,*

abra la lista desplegable en el sector izquierdo superior de la ventana **Configuración del área de protección** y seleccione **Vista de árbol**.

Los elementos o nodos se muestran en una visualización en forma de lista o en un modo de visualización en forma de árbol de los recursos del archivo del equipo de la siguiente manera:

 El nodo se incluye en el alcance de la protección.

 El nodo se excluye del alcance de la protección.

 Al menos uno de los nodos secundarios de este nodo se excluye del alcance de la protección, o la configuración de seguridad de los nodos secundarios difiere de la de un nodo principal (solo para el modo de visualización de vista de árbol).

El icono  se muestra si están seleccionados todos los nodos secundarios, pero no el principal. En este caso, los cambios en la composición de los archivos y las carpetas del nodo principal se ignoran automáticamente cuando el alcance de la protección para el nodo secundario seleccionado se está creando.

Utilizando la Consola de la aplicación, también puede agregar unidades virtuales (consulte la Sección "Creación del área virtual de protección" en la página 261) al alcance de la protección. Los nombres de los nodos virtuales se muestran en letras azules.

Configuración de seguridad

La configuración de seguridad de la tarea se puede ajustar como la configuración común para todos los nodos o elementos incluidos en el alcance de la protección, o como configuraciones diferentes para cada nodo o elemento en el árbol o lista del recurso del archivo del equipo.

La configuración de seguridad para el nodo principal seleccionado se aplica automáticamente a todos los nodos secundarios. La configuración de seguridad del nodo principal no se aplica a nodos secundarios que se configuran por separado.

La configuración de un alcance de la protección seleccionada se puede realizar mediante uno de los métodos siguientes:

- Seleccionar uno de tres niveles de seguridad predefinidos (en la página 233).
- Configuración manual de las opciones de seguridad (consulte la Sección "Configuración manual de las opciones de seguridad" en la página 246) para los nodos o elementos seleccionados en el árbol o lista de

recursos del archivo (el nivel de seguridad cambia a **Personalizado**).

Es posible guardar un conjunto de opciones de configuración para un nodo o elemento en una plantilla a fin de aplicarlo más tarde a otros nodos o elementos.

Acerca del área virtual de protección

Kaspersky Embedded Systems Security puede analizar no solo carpetas y archivos existentes en discos duros y unidades extraíbles, sino también unidades creadas dinámicamente en el equipo por distintas aplicaciones y servicios.

Si todos los objetos del equipo se incluyen en el alcance de la protección, estos nodos dinámicos se incluirán automáticamente en dicho alcance. No obstante, si desea especificar valores especiales para la configuración de seguridad de estos nodos dinámicos o si no ha seleccionado la protección en todo el equipo sino solo en áreas individuales, para incluir unidades, archivos o carpetas dinámicos en el alcance de la protección primero deberá crearlos en la consola de la aplicación: es decir, especificar el área virtual de protección. Las unidades, archivos y carpetas que se crearon existirán solo en la Consola de la aplicación, pero no en la estructura de archivos del equipo protegido.

Si, durante la creación de un alcance de la protección, se seleccionan todas las subcarpetas o archivos sin seleccionar la carpeta principal, todos los archivos o carpetas dinámicos que aparecerán en ella no se incluirán automáticamente en el alcance protegida. Se deben crear “copias virtuales” de ellos en la Consola de la aplicación y agregarlas al alcance de la protección.

Áreas de protección predefinidas

El árbol o la lista de recursos de archivos muestran los nodos a los cuales tiene acceso de lectura según la configuración de seguridad de Microsoft Windows.

Kaspersky Embedded Systems Security abarca las Áreas de protección predefinidas siguientes:

- **Discos duros locales**. Kaspersky Embedded Systems Security protege archivos en los discos duros del equipo.
- **Unidades extraíbles**. Kaspersky Embedded Systems Security protege archivos en dispositivos externos, por ejemplo, unidades USB o CD. Todas las unidades extraíbles, discos, carpetas o archivos individuales pueden incluirse o excluirse del alcance de la protección.
- **Red**. Kaspersky Embedded Systems Security analiza los archivos que se escriben en las carpetas de red o que son leídos por las aplicaciones que se ejecutan en el equipo. Kaspersky Embedded Systems Security no protege archivos cuando aplicaciones de otros equipos acceden a ellos.
- **Unidades virtuales**. Las unidades, archivos y carpetas dinámicos que se conectan temporalmente al equipo se pueden incluir en el alcance de la protección, por ejemplo, unidades de clústeres comunes.

De forma predeterminada, puede ver y configurar las áreas de protección predefinidas en el árbol de recursos de archivos en red; también puede agregar áreas de protección predefinidas a la lista de recursos de archivos en red durante su formación en la configuración del alcance de la protección.

De forma predeterminada, el alcance de la protección incluye todas las áreas predefinidas, excepto las unidades virtuales.

Las unidades virtuales creadas mediante un comando SUBST no se muestran en el árbol de recursos de archivo del equipo de la Consola de la aplicación. Para incluir objetos de la unidad virtual en el alcance de la protección, incluya la carpeta del equipo con la que se asocia la unidad virtual en el alcance de la protección.

Las unidades de red conectadas tampoco se mostrarán en la lista de recursos de archivos del equipo. Para incluir objetos de unidades de red en el alcance de la protección, especifique la ruta a la carpeta que corresponde a esta unidad de red en formato UNC.

Niveles de seguridad predefinidos

Se puede aplicar uno de los siguientes niveles de seguridad predefinidos para los nodos seleccionados en el árbol de recursos de archivos del equipo o la lista de recursos de archivo: **Máximo Rendimiento**, **Recomendado** y **Máxima Protección**. Cada uno de estos niveles contiene su propio conjunto de configuraciones de seguridad predefinidas (consulte la tabla a continuación).

Máximo Rendimiento

El nivel de seguridad **Máximo Rendimiento** se recomienda si, además del uso de Kaspersky Embedded Systems Security en los equipos, existen medidas adicionales de seguridad del equipo en la red, por ejemplo, si hay firewalls y directivas de seguridad existentes.

Recomendado

El nivel de seguridad **Recomendado** garantiza una óptima combinación de protección e impacto en el rendimiento de los equipos protegidos. Este nivel es recomendado por los expertos de Kaspersky Lab como suficiente para proteger equipos en la mayoría de las redes empresariales. El nivel de seguridad **Recomendado** está configurado de manera predeterminada.

Máxima Protección

Se recomienda el nivel de seguridad **Máxima Protección** si la red de la organización ha elevado los requisitos de seguridad del equipo.

Tabla 41. Niveles de seguridad predefinidos y valores de configuración correspondientes

Opciones	Nivel de seguridad		
	Máximo Rendimiento	Recomendado	Máxima Protección
Protección de objetos	Por extensión	Por formato	Por formato
Proteger solo los archivos nuevos y modificados	Habilitado	Habilitado	Deshabilitado
Acción que se realizará con los objetos infectados y otros objetos	Bloquear acceso y desinfectar. Eliminar si falla la desinfección	Bloquear acceso y realizar la acción recomendada	Bloquear acceso y desinfectar. Eliminar si falla la desinfección

Opciones	Nivel de seguridad		
Acción que se realizará con los objetos probablemente infectados	Bloquear acceso y colocar en Cuarentena	Bloquear acceso y realizar la acción recomendada	Bloquear acceso y colocar en Cuarentena
Excluir archivos	No	No	No
No detectar	No	No	No
Detener el análisis si demora más de (seg.)	60 segundos.	60 segundos.	60 segundos.
Omitir objetos compuestos de más de (MB)	8 MB	8 MB	Sin configurar
Analizar secuencias alternativas de NTFS	Sí	Sí	Sí
Analizar sectores de inicio del disco y MBR	Sí	Sí	Sí
Protección de objetos compuestos	• Objetos empaquetados* *Solo objetos nuevos y modificados	• Archivos SFX* • Objetos empaquetados* • Objetos OLE integrados* *Solo objetos nuevos y modificados	• Archivos SFX* • Objetos empaquetados* • Objetos OLE integrados* * Todos los objetos
Si se detecta un objeto integrado infectado, eliminar todo el archivo compuesto si la aplicación no puede modificarlo	No	No	Sí

Los parámetros **Protección de objetos**, **Usar la tecnología iChecker**, **Usar la tecnología iSwift** y **Usar el analizador heurístico** no se incluyen en la configuración de los niveles de seguridad predefinidos. Si modifica la configuración de seguridad de **Protección de objetos**, **Usar la tecnología iChecker**, **Usar la tecnología iSwift** o **Usar el analizador heurístico** después de seleccionar uno de los niveles de seguridad predefinidos, el nivel de seguridad que ha seleccionado no cambiará.

Extensiones de archivo analizadas de forma predeterminada en la tarea de Protección de archivos en tiempo real

De manera predeterminada, Kaspersky Embedded Systems Security analiza los archivos con las siguientes extensiones:

- *386;*
- *acm;*
- *ade, adp;*
- *asp;*
- *asx;*
- *ax;*
- *bas;*
- *bat;*
- *bin;*
- *chm;*
- *cla, clas*;*
- *cmd;*
- *com;*
- *cpl;*
- *crt;*
- *dll;*
- *dpl;*
- *drv;*
- *dvb;*
- *dwg;*
- *efi;*
- *emf;*
- *eml;*
- *exe;*
- *fon;*
- *fpm;*
- *hlp;*
- *hta;*
- *htm, html*;*

- *htt;*
- *ico;*
- *inf;*
- *ini;*
- *ins;*
- *isp;*
- *jpg, jpe;*
- *js, jse;*
- *lnk;*
- *mbx;*
- *msc;*
- *msg;*
- *msi;*
- *msp;*
- *mst;*
- *nws;*
- *ocx;*
- *oft;*
- *otm;*
- *pcd;*
- *pdf;*
- *php;*
- *pht;*
- *phtm*;*
- *pif;*
- *plg;*
- *png;*
- *pot;*
- *prf;*
- *prg;*
- *reg;*
- *rsc;*
- *rtf;*
- *scf;*
- *scr;*

- *sct;*
- *shb;*
- *shs;*
- *sht;*
- *shtm*;*
- *swf;*
- *sys;*
- *the;*
- *them*;*
- *tsp;*
- *url;*
- *vb;*
- *vbe;*
- *vbs;*
- *vxd;*
- *wma;*
- *wmf;*
- *wmv;*
- *wsc;*
- *wsf;*
- *wsh;*
- *do?;*
- *md?;*
- *mp?;*
- *ov?;*
- *pp?;*
- *vs?;*
- *xl?.*

Configuración de la tarea Protección de archivos en tiempo real predeterminada

De manera predeterminada, la tarea de Protección de archivos en tiempo real utiliza la configuración descrita en la siguiente tabla. Puede cambiar los valores de esta configuración.

Tabla 42. Configuración de la tarea Protección de archivos en tiempo real predeterminada

Configuración	Valor predeterminado	Descripción
Área de protección	El equipo completo, excluidas las unidades virtuales.	Se puede limitar el alcance de la protección.
Modo de protección de objetos	**Al acceder y realizar modificaciones**	Puede seleccionar el modo de protección, es decir, definir el tipo de acceso en el que Kaspersky Embedded Systems Security analizará los objetos.
Analizador heurístico	Se aplica el nivel de seguridad **Medio**.	Se puede habilitar o deshabilitar el Analizador heurístico y se puede configurar el nivel de análisis.
Aplicar la Zona de confianza	Aplicado.	Lista general de exclusiones que se puede utilizar en tareas seleccionadas.
Usar KSN para protección	Aplicado.	Puede mejorar la protección del servidor con la infraestructura de servicios en la nube de Kaspersky Security Network (disponible si se acepta la Declaración de KSN).
Programación de inicio de tareas	Al inicio de la aplicación.	Puede configurar el inicio de la tarea programado.
Bloquear acceso a recursos compartidos en la red para los hosts que muestran actividad maliciosa	No aplicado.	Puede agregar hosts que muestren actividad maliciosa a la lista de hosts bloqueados.

Gestión de la tarea Protección de archivos en tiempo real a través del Complemento de administración

En esta sección, aprenderá a navegar la interfaz del Complemento de administración y ajustar la configuración de la tarea para uno o todos los equipos en la red.

En esta sección

Navegación

Sepa cómo navegar a la configuración de la tarea requerida a través de la interfaz.

En esta sección

Cómo abrir la configuración de la directiva para la tarea Protección de archivos en tiempo real

► *Para abrir la configuración de la tarea Protección de archivos en tiempo real a través de la directiva Kaspersky Security Center:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas.**
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Protección del equipo en tiempo real**.
6. Haga clic en el botón **Configurar** en la subsección **Protección de archivos en tiempo real**.

   Se abre la ventana **Protección de archivos en tiempo real**.

Si un equipo es administrado por una directiva activa de Kaspersky Security Center y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede editar a través de la Consola de la aplicación.

Cómo abrir las propiedades de la tarea Protección de archivos en tiempo real

► *Para abrir la ventana de configuración de la tarea Protección de archivos en tiempo real para un solo equipo en red:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Dispositivos**.

4. Abra la ventana **Propiedades: <Nombre del equipo>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre del equipo protegido
   - Seleccione el elemento **Propiedades** en el menú contextual del equipo protegido.

   Se abre la ventana **Propiedades:** Se abre la ventana **<Nombre del equipo>**.
5. En la sección **Tareas**, seleccione la tarea **Protección de archivos en tiempo real**.
6. Haga clic en el botón **Propiedades**.

   Se abre la ventana **Propiedades:** Se abre la ventana **Protección de archivos en tiempo real**.

Configuración de la tarea Protección de archivos en tiempo real

► *Para establecer la configuración de la tarea Protección de archivos en tiempo real:*

1. Abra la ventana **Protección de archivos en tiempo real** (consulte la Sección "Cómo abrir la configuración de la directiva para la tarea Protección de archivos en tiempo real" en la página 239).
2. Defina los siguientes valores de configuración de tarea:
   - En la pestaña **General**:
     - **Modo de protección de objetos** (consulte la sección "**Selección del modo de protección**", en la página 241)
     - **Analizador heurístico**
     - **Integración con otros componentes** (consulte la sección "**Configuración del Analizador heurístico e integración con otros componentes de la aplicación**" en la página 242)
   - En la pestaña **Administración de la tarea**:
     - Opciones de programación de inicio de tareas (consulte la sección “Configuración de las opciones de programación de inicio de tareas”, en la página 128).
3. Seleccione la pestaña **Área de protección** y haga lo siguiente:
   - Haga clic en el botón **Agregar** o **Editar** para editar el alcance de la protección (consulte la sección “Creación del alcance de la protección”, en la página 258).
     - En la ventana que se abre, elija lo que desea incluir en el alcance de la protección de la tarea:
       - **Área predefinida**
       - **Disco, carpeta o ubicación de red**
       - **Archivo**
     - Seleccione uno de los niveles de seguridad predefinidos (en la página 233) o configure manualmente las opciones de protección (consulte la sección “Configuración manual de las opciones de protección”, en la página 246).
4. Haga clic en **Aceptar** en la ventana **Protección de archivos en tiempo real**.

Kaspersky Embedded Systems Security aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

En esta sección

Selección del modo de protección

En la tarea Protección de archivos en tiempo real, se puede seleccionar el modo de protección. La sección **Modo de protección de objetos** le permite especificar el tipo de acceso a objetos que Kaspersky Embedded Systems Security debería analizar.

El parámetro **Modo de protección de objetos** tiene el valor común para todo el alcance de la protección especificada en la tarea. No es posible especificar valores diferentes en el parámetro para nodos individuales dentro del alcance de la protección.

► *Para seleccionar el modo de protección:*

1. Abra la ventana **Protección de archivos en tiempo real** (consulte la Sección "Cómo abrir la configuración de la directiva para la tarea Protección de archivos en tiempo real" en la página 239).
2. En la ventana que se abre, abra la pestaña **General** y seleccione el modo de protección que desea configurar:
   - **Modo inteligente**

     Kaspersky Embedded Systems Security selecciona objetos para analizar por su cuenta. El objeto se analiza cuando se abre y, luego, nuevamente después de guardarlo si se modificó. Si el proceso realizó varias llamadas al objeto mientras se estaba ejecutando y si el proceso lo modificó, Kaspersky Embedded Systems Security analiza el objeto de nuevo solo después de que el proceso lo guarda por última vez.
   - **Al acceder y realizar modificaciones**

     Kaspersky Embedded Systems Security analiza el objeto cuando se abre y vuelve a analizarlo después de que se guarda si el objeto se modifica.

     De forma predeterminada, esta opción está seleccionada.
   - **Al acceder**

     Kaspersky Embedded Systems Security analiza todos los objetos cuando se abren para su lectura, ejecución o modificación.
   - **Durante ejecución**

     Kaspersky Embedded Systems Security analiza el archivo solo cuando se accede para su ejecución.
3. Haga clic en **Aceptar**.

Se aplicará el modo de protección seleccionado.

Configuración del Analizador heurístico e integración con otros componentes de la aplicación

Para iniciar la tarea Uso de KSN, debe aceptar la Declaración de Kaspersky Security Network.

► *Para configurar el Analizador heurístico y la integración con otros componentes:*

1. Abra la ventana **Protección de archivos en tiempo real** (consulte la Sección "Cómo abrir la configuración de la directiva para la tarea Protección de archivos en tiempo real" en la página 239).
2. En la pestaña **General**, desactive o seleccione la casilla de verificación **Usar el analizador heurístico**.

   Esta casilla de verificación habilita y deshabilita el Analizador heurístico durante el análisis de objetos.

   Si la casilla está activada, el Analizador heurístico está habilitado.

   Si la casilla está desactivada, el Analizador heurístico está deshabilitado.

   De forma predeterminada, la casilla está activada.
3. Si es necesario, ajuste el nivel de análisis con el control deslizante.

   El control deslizante le permite ajustar el nivel del análisis heurístico. El nivel de intensidad del análisis ofrece un equilibrio entre la profundidad de las búsquedas de nuevas amenazas, el consumo de recursos del sistema operativo y el tiempo requerido para el análisis.

   Los siguientes niveles de intensidad del análisis están disponibles:

   - **Ligero**. El analizador heurístico realiza menos operaciones encontradas en archivos ejecutables. La probabilidad de detección de amenazas en este modo es en cierto grado inferior. El análisis es más rápido y consume menos recursos.
   - **Medio**. El Analizador heurístico realiza el número de instrucciones encontradas en los archivos ejecutables recomendados por los expertos de Kaspersky Lab.

     Este nivel está seleccionado de forma predeterminada.
   - **Profundo**. El analizador heurístico realiza más operaciones encontradas en archivos ejecutables. La probabilidad de detección de amenazas en este modo es mayor. El análisis consume más recursos del sistema, lleva más tiempo y puede causar un número más alto de falsas alarmas.

     El control deslizante está disponible si la casilla **Usar el analizador heurístico** está seleccionada.
4. En la sección **Integración con otros componentes**, configure las siguientes opciones:
   - Seleccione o desactive la casilla de verificación **Aplicar la Zona de confianza**.

     Esta casilla de verificación habilita y deshabilita el uso de la Zona de confianza para una tarea.

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security agrega operaciones del archivo de procesos de confianza a las exclusiones de análisis configuradas en la tarea.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security ignora las operaciones del archivo de procesos de confianza al formar el alcance de la protección para la tarea.

     De forma predeterminada, la casilla está activada.

- Seleccione o desactive la casilla de verificación **Usar KSN para protección**.

  Esta casilla de verificación habilita o deshabilita el uso de servicios de KSN.

  Si se selecciona la casilla, la aplicación utiliza los datos de Kaspersky Security Network para asegurarse de que la aplicación responda con mayor rapidez a amenazas nuevas y para reducir la posibilidad de falsos positivos.

  Si la casilla de verificación está desactivada, la tarea no usa los servicios de KSN.

  De forma predeterminada, la casilla está activada.

  La casilla de verificación **Enviar datos sobre archivos analizados** debe estar seleccionada en la configuración de la tarea Uso de KSN.

- Seleccione o desactive la casilla de verificación **Bloquear acceso a recursos compartidos en la red para los hosts que muestran actividad maliciosa**.

5. Haga clic en **Aceptar**.

La configuración de la tarea se aplica inmediatamente a la tarea en ejecución. Si la tarea no se está ejecutando, la configuración modificada se aplica en el siguiente inicio.

Configuración de las opciones de programación de inicio de tareas

Puede configurar la programación de inicio de las tareas personalizadas y del sistema local en la Consola de la aplicación. No puede configurar la programación de inicio de tareas de grupo.

► *Para configurar las opciones de programación de inicio de tareas de grupo, siga estos pasos:*

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.
2. Seleccione el grupo al cual pertenece el servidor protegido.
3. En el panel de detalles, seleccione la pestaña **Tareas**.
4. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea.
   - Abra el menú contextual del nombre de la tarea y seleccione el elemento Propiedades
5. Seleccione la sección **Programación**.
6. En el bloque **Configuración de programación**, seleccione la casilla de verificación **Ejecutar según programación**.

   Los campos con la configuración de programación para la tarea Análisis a pedido y la tarea Actualización no estarán disponibles si el inicio programado está bloqueado por una directiva de Kaspersky Security Center.

7. Configure los valores de programación de acuerdo con sus requisitos. Para ello, realice las siguientes acciones:
   a. En la lista **Frecuencia**, seleccione uno de los siguientes valores:
      - **Horaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de horas;

especifique el número de horas en el campo **Cada <número> hora(s)**.

- **Diaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de días; especifique el número de horas en el campo **Cada <número> día(s)**.
- **Semanal**, si desea que la tarea se ejecute con intervalos durante un número especificado de semanas; especifique el número de horas en el campo **Cada <número> semana(s)**. Especifique los días de la semana durante los cuales la tarea se iniciará (de manera predeterminada, las tareas se ejecutan los lunes).
- **Al inicio de la aplicación**, si desea que la tarea se ejecute cada vez que se inicia Kaspersky Embedded Systems Security.
- **Tras la actualización de bases de datos de la aplicación**, si desea que la tarea se ejecute después de cada actualización de bases de datos de la aplicación.

b. Especifique la hora del primer inicio de la tarea en el campo **Hora de inicio**.

c. En el campo **Fecha de inicio**, especifique la fecha desde la que se aplicará la programación.

Después de especificar la frecuencia de inicio de la tarea, la hora del primer inicio de esta y la fecha desde la que se aplicará la programación, la información sobre la hora calculada para el próximo inicio de la tarea se mostrará en la parte superior de la ventana en el campo **Próximo inicio**. La información actualizada sobre la hora estimada del próximo inicio de la tarea se mostrará cada vez que abra la ventana **Configuración de tareas** de la pestaña **Programación**. El valor **Bloqueado por directiva** se muestra en el campo **Próximo inicio** si la configuración de la directiva activa de Kaspersky Security Center prohíbe el inicio de tareas programadas del sistema (consulte la sección “Configuración del inicio programado de las tareas locales del sistema”, en la página 96).

8. Use la pestaña **Avanzado** para configurar las siguientes opciones de programación de acuerdo con sus requisitos.
   - En la sección **Configuración de detención de la tarea**:
     a. Seleccione la casilla de verificación **Duración** y escriba el número requerido de horas y minutos en los campos a la derecha para especificar la duración máxima de la ejecución de la tarea.
     b. Seleccione la casilla de verificación **Pausar de** y escriba los valores de inicio y de finalización del intervalo de tiempo en los campos a la derecha para especificar el intervalo de tiempo inferior a 24 horas durante el cual la ejecución de la tarea se pausará.
   - En la sección **Configuración avanzada**:
     a. Seleccione la casilla de verificación **Fin de la programación** y especifique la fecha desde la cual la programación dejará de funcionar.
     b. Seleccione la casilla de verificación **Ejecutar tareas omitidas** para habilitar el inicio de las tareas omitidas.
     c. Seleccione la casilla de verificación **Aleatorizar la hora de inicio de la tarea usando un margen de** y especifique el valor en minutos.
9. Haga clic en **Aceptar**.
10. Haga clic en el botón **Aplicar** para guardar la configuración del inicio de la tarea.

Si desea establecer la configuración de la aplicación para una sola tarea con Kaspersky Security Center, realice los pasos que se detallan en Configuración de tareas locales en la ventana de configuración de la aplicación de la sección Kaspersky Security Center (en la página 117).

Creación y configuración del alcance de la protección de la tarea

► *Para crear y configurar el alcance de la protección de la tarea a través de Kaspersky Security Center:*

1. Abra la ventana **Protección de archivos en tiempo real** (consulte la Sección "Cómo abrir la configuración de la directiva para la tarea Protección de archivos en tiempo real" en la página 239).
2. Seleccione la pestaña **Área de protección**.
3. Todos los elementos ya protegidos por la tarea se enumeran en la tabla **Área de protección**.
4. Haga clic en el botón **Agregar** para agregar el nuevo elemento a la lista.

   Se abre la ventana **Agregar objetos al área de protección**.
5. Seleccione un tipo de objeto para agregarlo a un alcance de la protección:
   - **Área predefinida** para incluir una de las áreas predefinidas en el alcance de la protección en el servidor. A continuación, en la lista desplegable, seleccione un alcance de la protección necesaria.
   - **Disco, carpeta o ubicación de red** para incluir una unidad individual, carpeta o un objeto de red en un alcance de la protección. A continuación, seleccione un alcance de la protección necesaria con un clic en el botón **Examinar**.
   - **Archivo** para incluir un archivo particular en el alcance de la protección. A continuación, seleccione un alcance de la protección necesaria con un clic en el botón **Examinar**.

     No puede agregar un objeto al alcance de la protección si ya se agregó como una exclusión de un alcance de la protección.
6. Para excluir elementos individuales del alcance de la protección, desactive las casillas al lado de los nombres de estos elementos o siga estos pasos:
   a. Abra el menú contextual del alcance de la protección haciendo clic en él con el botón derecho del mouse.
   b. En el menú contextual, seleccione la opción **Agregar exclusión**.
   c. En la ventana **Agregar exclusión**, seleccione un tipo de objeto que desee agregar como una exclusión del alcance de la protección siguiendo la lógica del objeto agregado a un procedimiento de alcance de la protección.
7. Para modificar el alcance de la protección o una exclusión agregada, seleccione la opción **Editar área** en el menú contextual del alcance de la protección necesaria.
8. Para ocultar el alcance de la protección agregada anteriormente o una exclusión en la lista de recursos de archivos en red, seleccione la opción **Eliminar área** en el menú contextual del alcance de la protección necesaria.

El alcance de la protección se excluye del alcance de la tarea de Protección de archivos en tiempo real al ser eliminada de la lista de recursos de archivos en red.

9. Haga clic en el botón **Guardar**.

La ventana de la configuración del alcance de la protección se cierra. Se guardan las opciones configuradas recientemente.

La tarea de **Protección de archivos en tiempo real** puede iniciarse solo si al menos uno de los nodos de recursos de archivos del equipo se incluye en un alcance de la protección.

Configuración manual de las opciones de seguridad

De manera predeterminada, la tarea de Protección de archivos en tiempo real utiliza la configuración de seguridad común para todo el alcance de la protección. Estos ajustes corresponden a los del nivel de seguridad predefinido **Recomendado** (consulte la sección “Niveles de seguridad predefinidos”, en la página 233).

Los valores predeterminados de la configuración de seguridad se pueden modificar configurándolos como valores comunes para todo el alcance de la protección, o como valores diferentes para los diversos elementos de la lista de recursos de archivos del equipo o nodos del árbol.

► *Para configurar las opciones de seguridad del nodo seleccionado en forma manual:*

1. Abra la ventana **Protección de archivos en tiempo real** (consulte la Sección "Cómo abrir la configuración de la directiva para la tarea Protección de archivos en tiempo real" en la página 239).
2. En la pestaña **Área de protección**, seleccione el nodo cuya configuración de seguridad desea configurar y hacer clic en **Configurar**.

   La ventana **Configuración de Protección de archivos en tiempo real** se abre.
3. En la pestaña **Nivel de seguridad**, haga clic en el botón **Configurar** para establecer la configuración personalizada.
4. Puede configurar los valores de seguridad requeridos del nodo seleccionado de acuerdo con sus requisitos:
   - Configuración general (consulte la sección “Configuración general de las opciones de tareas”, en la página 247)
   - Acciones (consulte la sección “Configuración de acciones”, en la página 249)
   - Rendimiento (consulte la sección “Configuración de rendimiento”, en la página 251)
5. Haga clic en **Aceptar** en la ventana **Protección de archivos en tiempo real**.

Se guarda la nueva configuración del alcance de la protección.

En esta sección

Configuración de las opciones generales de tareas

► *Para configurar las opciones de seguridad generales de la tarea Protección de archivos en tiempo real:*

1. Abra la ventana **Configuración de Protección de archivos en tiempo real** (consulte la Sección "Cómo abrir la configuración de la directiva para la tarea Protección de archivos en tiempo real" en la página 239).
2. Seleccione la pestaña **General**.
3. En la sección **Protección de objetos**, especifique los tipos de objetos que desea incluir en el alcance de la protección:
   - **Todos los objetos**

     Kaspersky Embedded Systems Security analiza todos los objetos.
   - **Objetos analizados según su formato**

     Kaspersky Embedded Systems Security solo analiza los objetos infectables según el formato del archivo.

     Kaspersky Lab compila la lista de formatos. Se incluye en las bases de datos de Kaspersky Embedded Systems Security.
   - **Objetos analizados según la lista de extensiones de la base de datos antivirus**

     Kaspersky Embedded Systems Security solo analiza los objetos infectables según la extensión del archivo.

     Kaspersky Lab compila la lista de extensiones. Se incluye en las bases de datos de Kaspersky Embedded Systems Security.
   - **Objetos analizados según la lista de extensiones especificada**

     Kaspersky Embedded Systems Security analiza los archivos según su extensión. La lista de extensiones de archivos se puede personalizar manualmente en la ventana **Lista de extensiones**, que se puede abrir con un clic en el botón **Editar**.
   - **Analizar sectores de inicio del disco y MBR**

     Habilita la protección de los sectores de inicio y los registros de inicio maestros.

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los sectores de inicio y los registros de inicio maestro en los discos duros y las unidades extraíbles del equipo.

     De forma predeterminada, la casilla está activada.
   - **Analizar secuencias alternativas de NTFS**

     Análisis de flujos de archivos y carpetas alternativos en las unidades del sistema de archivos NTFS.

     Si se selecciona la casilla de verificación, la aplicación analiza un objeto probablemente

infectado y todos los flujos NTFS asociados con ese objeto.

Si se cancela la selección de la casilla de verificación, la aplicación solo analiza el objeto que se detectó y se consideró como probablemente infectado.

De forma predeterminada, la casilla está activada.

4. En la sección **Rendimiento**, seleccione o cancele la selección de la casilla de verificación **Proteger solo los archivos nuevos y modificados**.

   Esta casilla de verificación activa y desactiva el análisis y la protección de archivos que Kaspersky Embedded Systems Security reconoció como nuevos o modificados desde el último análisis.

   Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza y protege solo los archivos que reconoció como nuevos o modificados desde el último análisis.

   Si se cancela la selección de la casilla de verificación, puede seleccionar si desea analizar y proteger solo archivos nuevos o todos los archivos, más allá de su estado de modificación.

   De forma predeterminada, la casilla está activada para el nivel de seguridad **Máximo Rendimiento**. Si se configuran los niveles de seguridad **Máxima Protección** o **Recomendado**, la casilla de verificación se desactiva.

   Para cambiar entre opciones disponibles cuando la casilla está desactivada, haga clic en el vínculo **Todos** / **Solo nuevos** para cada uno de los tipos de objeto compuestos.

5. En la sección **Protección de objetos compuestos**, especifique los objetos compuestos que desea incluir en el alcance de la protección:

   - **Todos/Solo nuevos archivos comprimidos**

     Análisis de archivos ZIP, CAB, RAR, ARJ y otros formatos de archivos.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los archivos comprimidos.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos comprimidos durante el análisis.

     El valor predeterminado depende del nivel de protección seleccionado.

   - **Todos/Solo nuevos archivos SFX**

     Análisis de archivos autoextraíbles.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza archivos SFX.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos SFX durante el análisis.

     El valor predeterminado depende del nivel de protección seleccionado.

     Esta opción se encuentra activa cuando la casilla de verificación **Archivos comprimidos** está desactivada.

   - **Todos/Solo nuevas bases de datos de correo electrónico**

     Análisis de archivos de bases de datos de correo de Microsoft Outlook y Microsoft Outlook Express.

Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza todos los archivos de la base de datos de correo.

Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos de la base de datos de correo durante el análisis.

El valor predeterminado depende del nivel de seguridad seleccionado.

- **Todos/Solo nuevos objetos empaquetados**

  Análisis de archivos ejecutables empaquetados mediante compresores de código binario, tales como UPX o ASPack.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los archivos ejecutables empaquetados por empaquetadores.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos ejecutables empaquetados por empaquetadores durante el análisis.

  El valor predeterminado depende del nivel de protección seleccionado.

- **Todos/Solo nuevo correo electrónico simple**

  Análisis de archivos de formatos de correo, tales como mensajes de Microsoft Outlook y Microsoft Outlook Express.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los archivos con formato de correo.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos con formato de correo durante el análisis.

  El valor predeterminado depende del nivel de seguridad seleccionado.

- **Todos/Solo nuevos objetos OLE incorporados**

  Análisis de objetos integrados en archivos (por ejemplo, macros de Microsoft Word o archivos adjuntos del mensaje de correo electrónico).

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los objetos integrados en archivos.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los objetos integrados en archivos durante el análisis.

  El valor predeterminado depende del nivel de protección seleccionado.

6. Haga clic en **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de acciones

► *Para configurar las acciones en objetos infectados y otros objetos detectados para la tarea de Protección de archivos en tiempo real:*

1. Abra la ventana **Configuración de Protección de archivos en tiempo real**(consulte la Sección "**Cómo abrir la configuración de la directiva para la tarea Protección de archivos en tiempo real**" en la página 239).
2. Seleccione la pestaña **Acciones**.

3. Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:

   - **Solo notificar**.

     Cuando se selecciona este modo, Kaspersky Embedded Systems Security no bloquea el acceso a los objetos infectados y a otros objetos detectados ni realiza ninguna acción relacionada con ellos. Se registra el siguiente evento en el registro de tareas: *Objeto no desinfectado. Motivo: No se tomó ninguna acción para neutralizar el objeto detectado debido a la configuración definida por el usuario.* El evento especifica toda la información disponible sobre el objeto detectado.

     El modo **Solo notificar** debe configurarse por separado para cada área de protección o análisis. Este modo no se usa de forma predeterminada en ninguno de los niveles de seguridad. Si selecciona este modo, Kaspersky Embedded Systems Security cambia automáticamente el nivel de seguridad a **Personalizado**.

   - **Bloquear acceso**.

     Cuando se selecciona esta opción, Kaspersky Embedded Systems Security bloquea el acceso al objeto detectado o probablemente infectado. Puede seleccionar una acción adicional sobre los objetos bloqueados en la lista desplegable.

   - **Realizar acción adicional**.

     Seleccione la acción en la lista desplegable:

     - **Desinfectar**.
     - **Desinfectar. Desinfectar; si falla la desinfección, eliminar**.
     - **Eliminar**.
     - **Recomendado**.

4. Seleccione la acción a realizar en los objetos probablemente infectados:

   - **Solo notificar**.

     Cuando se selecciona este modo, Kaspersky Embedded Systems Security no bloquea el acceso a los objetos infectados y a otros objetos detectados ni realiza ninguna acción relacionada con ellos. Se registra el siguiente evento en el registro de tareas: *Objeto no desinfectado. Motivo: No se tomó ninguna acción para neutralizar el objeto detectado debido a la configuración definida por el usuario.* El evento especifica toda la información disponible sobre el objeto detectado.

     El modo **Solo notificar** debe configurarse por separado para cada área de protección o análisis. Este modo no se usa de forma predeterminada en ninguno de los niveles de seguridad. Si selecciona este modo, Kaspersky Embedded Systems Security cambia automáticamente el nivel de seguridad a **Personalizado**.

   - **Bloquear acceso**.

     Cuando se selecciona esta opción, Kaspersky Embedded Systems Security bloquea el acceso al objeto detectado o probablemente infectado. Puede seleccionar una acción adicional sobre los objetos bloqueados en la lista desplegable.

   - **Realizar acción adicional**.

     Seleccione la acción en la lista desplegable:

     - **Poner en cuarentena**.
     - **Eliminar**.

- **Recomendado**.

5. Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:
   a. Borre o seleccione la casilla de verificación **Realizar acciones según el tipo de objeto detectado**.

      Si se selecciona la casilla, puede configurar independientemente la acción principal y secundaria para cada tipo de objeto detectado haciendo clic en el botón **Configurar** ubicado junto a la casilla de verificación. En ese momento, Kaspersky Embedded Systems Security no permitirá abrir o ejecutar un objeto infectado, independientemente de su elección.

      Si la casilla de verificación no está seleccionada, Kaspersky Embedded Systems Security realiza las acciones seleccionadas en las secciones **Acción que se realizará con los objetos infectados y otros objetos** y **Acción que se realizará con los objetos probablemente infectados** para los tipos de objetos correspondientes.

      De forma predeterminada, la casilla está desactivada.

   b. Haga clic en el botón **Configurar**.
   c. En la ventana que se abre, seleccione la acción primaria y secundaria (en caso de que falle la primaria) para cada tipo de objeto detectado.
   d. Haga clic en **Aceptar**.
6. Seleccione la acción a realizar en archivos compuestos no modificables: seleccione o borre la casilla de verificación **Si se detecta un objeto integrado infectado, eliminar todo el archivo compuesto si la aplicación no puede modificarlo**.

   Esta casilla habilita o deshabilita la eliminación forzada del archivo compuesto principal cuando se detecta un objeto secundario malicioso, probablemente infectado u otro objeto secundario integrado.

   Si se selecciona la casilla de verificación y se configura la tarea para eliminar los objetos infectados y probablemente infectados. Kaspersky Embedded Systems Security elimina de manera forzada todo el objeto compuesto principal cuando se detecta un objeto malicioso u otro objeto integrado. La eliminación forzada de un archivo principal junto con todo su contenido sucede si la aplicación no puede eliminar únicamente el objeto secundario detectado (por ejemplo, si el objeto principal es inmodificable).

   Si se desactiva esta casilla y la tarea se configura para eliminar objetos infectados y probablemente infectados, Kaspersky Embedded Systems Security no realiza la acción seleccionada si el objeto principal es inmodificable.
7. Haga clic en **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de rendimiento

► *Para configurar el rendimiento para la tarea Protección de archivos en tiempo real:*

1. Abra la ventana **Configuración de Protección de archivos en tiempo real (consulte la Sección "Cómo abrir la configuración de la directiva para la tarea Protección de archivos en tiempo real" en la página** 239**)**.
2. Seleccione la pestaña **Rendimiento**.

3. En la sección **Exclusiones**:
   - Borre o seleccione la casilla de verificación **Excluir archivos**.

     Excluir archivos del análisis por nombre de archivo o máscara de nombre de archivo.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos especificados durante el análisis.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza todos los objetos.

     De forma predeterminada, la casilla está desactivada.
   - Borre o seleccione la casilla de verificación **No detectar**.

     Los objetos se excluyen del análisis por el nombre o la máscara del nombre del objeto detectable. La lista de nombres de objetos detectables está disponible en el sitio web de la Enciclopedia de Virus https://encyclopedia.kaspersky.com/knowledge/classification/

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos especificados detectables durante el análisis.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security detecta todos los objetos especificados en la aplicación de forma predeterminada.

     De forma predeterminada, la casilla está desactivada.
   - Haga clic en el botón **Editar** en cada para parámetro agregar exclusiones.
4. En la sección **Configuración avanzada**:
   - **Detener el análisis si demora más de (seg.)**

     Limita la duración del análisis de objetos. El valor predeterminado es 60 segundos.

     Si la casilla está desactivada, la duración del análisis se limita al valor especificado.

     Si la casilla está desactivada, la duración del análisis es ilimitada.

     De forma predeterminada, la casilla está activada para el nivel de seguridad **Máximo Rendimiento**.
   - **Omitir objetos compuestos de más de (MB)**

     Excluye del análisis objetos más grandes que el tamaño especificado.

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos compuestos cuyo tamaño supera el límite especificado durante el análisis antivirus.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza los objetos compuestos de cualquier tamaño.

     De forma predeterminada, la casilla está activada para el nivel de seguridad **Máximo Rendimiento**.
   - **Usar la tecnología iSwift**

     iSwift compara el identificador NTFS del archivo, que está almacenado en una base de datos, con un identificador actual. El análisis se realiza solo para archivos cuyos identificadores han cambiado (archivos nuevos y archivos modificados desde el último análisis de objetos del sistema NTFS).

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security solo analiza los archivos nuevos o modificados desde el último análisis de objetos del

sistema NTFS.

Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza los objetos del sistema del archivo NTFS sin considerar la fecha de creación o modificación del archivo, excepto los archivos de carpetas de red.

De forma predeterminada, la casilla está activada.

- **Usar la tecnología iChecker**

  iChecker calcula y recuerda las sumas de control de los archivos analizados. Si un objeto se modifica, la suma de control cambia. La aplicación compara todas las sumas de control durante la tarea de análisis, y analiza solo los archivos nuevos y modificados desde el último análisis.

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza solo los archivos nuevos y modificados.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza los archivos sin considerar la fecha de creación o modificación del archivo.

  De forma predeterminada, la casilla está activada.

Gestión de la tarea de Protección de archivos en tiempo real a través de la Consola de la aplicación

En esta sección, aprenda a navegar la interfaz de la Consola de la aplicación y establecer la configuración de la tarea en un equipo local.

En esta sección

Navegación

Sepa cómo navegar a la configuración de la tarea requerida a través de la interfaz.

Cómo abrir la configuración del alcance de la Protección de archivos en tiempo real

► *Para abrir la ventana de configuración del alcance de la protección de la tarea Protección de archivos en tiempo real:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Protección de archivos en tiempo real**.
3. Haga clic en el vínculo **Configurar el área de protección** en el panel de detalles.

   Se abre la ventana **Configuración del área de protección**.

Cómo abrir la configuración de la tarea Protección de archivos en tiempo real

► *Para abrir la ventana de la configuración de la tarea general:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Protección de archivos en tiempo real**.
3. Haga clic en el vínculo **Propiedades** del panel de detalles.

   Se abre la ventana **Configuración de tareas**.

Configuración de la tarea Protección de archivos en tiempo real

► *Para establecer la configuración de la tarea Protección de archivos en tiempo real:*

1. Abra la ventana **Configuración de tareas** (consulte la sección “Cómo abrir la configuración de la tarea Protección de archivos en tiempo real” en la página 254).
2. En la pestaña **General**, configure la siguiente configuración de tarea:
   - **Modo de protección de objetos** (consulte la sección "**Selección del modo de protección**", en la página 255)
   - **Analizador heurístico**
   - **Integración con otros componentes** (consulte la sección "**Configuración del Analizador heurístico e integración con otros componentes de la aplicación**" en la página 256)
3. En las pestañas **Programación** y **Avanzado**, especifique las opciones de inicio programado (consulte la sección "Configuración de las opciones de programación de inicio de tareas" en la página 149).
4. Haga clic en **Aceptar** en la ventana **Configuración de tareas**.

   La configuración modificada se guarda.
5. En el panel de detalles del nodo **Protección de archivos en tiempo real**, haga clic en el vínculo **Configurar el área de protección**.
6. Haga lo siguiente:
   - En el árbol o en la lista de recursos del archivo del equipo, seleccione los nodos o elementos que desea incluir en el alcance de la protección de la tarea.

- Seleccione uno de los niveles de seguridad predefinidos o ajuste la configuración de protección de objeto manualmente (consulte la Sección "Configuración manual de las opciones de seguridad" en la página 431).

7. En la ventana **Configuración del área de protección**, haga clic en el botón **Guardar**.

Kaspersky Embedded Systems Security aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea se establecen antes y después de la modificación, se guardan en el registro de auditoría del sistema.

En esta sección

Selección del modo de protección

En la tarea Protección de archivos en tiempo real, se puede seleccionar el modo de protección. La sección **Modo de protección de objetos** le permite especificar el tipo de acceso a objetos que Kaspersky Embedded Systems Security debería analizar.

El parámetro **Modo de protección de objetos** tiene el valor común para todo el alcance de la protección especificada en la tarea. No es posible especificar valores diferentes en el parámetro para nodos individuales dentro del alcance de la protección.

► *Para seleccionar el modo de protección, siga estos pasos:*

1. Abra la ventana **Configuración de tareas** (consulte la sección “Cómo abrir la configuración de la tarea Protección de archivos en tiempo real” en la página 254).
2. En la ventana que se abre, abra la pestaña **General** y seleccione el modo de protección que desea configurar:
   - **Modo inteligente**

     Kaspersky Embedded Systems Security selecciona objetos para analizar por su cuenta. El objeto se analiza cuando se abre y, luego, nuevamente después de guardarlo si se modificó. Si el proceso realizó varias llamadas al objeto mientras se estaba ejecutando y si el proceso lo modificó, Kaspersky Embedded Systems Security analiza el objeto de nuevo solo después de que el proceso lo guarda por última vez.
   - **Al acceder y realizar modificaciones**

     Kaspersky Embedded Systems Security analiza el objeto cuando se abre y vuelve a analizarlo después de que se guarda si el objeto se modifica.

     De forma predeterminada, esta opción está seleccionada.
   - **Al acceder**

     Kaspersky Embedded Systems Security analiza todos los objetos cuando se abren para su lectura, ejecución o modificación.
   - **Durante ejecución**

Kaspersky Embedded Systems Security analiza el archivo solo cuando se accede para su ejecución.

3. Haga clic en **Aceptar**.

Se aplicará el modo de protección seleccionado.

Configuración del Analizador heurístico e integración con otros componentes de la aplicación

Para iniciar la tarea Uso de KSN, debe aceptar la Declaración de Kaspersky Security Network.

► *Para configurar el Analizador heurístico y la integración con otros componentes:*

1. Abra la ventana **Configuración de tareas** (consulte la sección "**Cómo abrir la configuración de la tarea Protección de archivos en tiempo real**" en la página 254).
2. En la pestaña **General**, desactive o seleccione la casilla de verificación **Usar el analizador heurístico**.

   Esta casilla de verificación habilita y deshabilita el Analizador heurístico durante el análisis de objetos.

   Si la casilla está activada, el Analizador heurístico está habilitado.

   Si la casilla está desactivada, el Analizador heurístico está deshabilitado.

   De forma predeterminada, la casilla está activada.
3. Si es necesario, ajuste el nivel de análisis con el control deslizante.

   El control deslizante le permite ajustar el nivel del análisis heurístico. El nivel de intensidad del análisis ofrece un equilibrio entre la profundidad de las búsquedas de nuevas amenazas, el consumo de recursos del sistema operativo y el tiempo requerido para el análisis.

   Los siguientes niveles de intensidad del análisis están disponibles:

   - **Ligero**. El analizador heurístico realiza menos operaciones encontradas en archivos ejecutables. La probabilidad de detección de amenazas en este modo es en cierto grado inferior. El análisis es más rápido y consume menos recursos.
   - **Medio**. El Analizador heurístico realiza el número de instrucciones encontradas en los archivos ejecutables recomendados por los expertos de Kaspersky Lab.

     Este nivel está seleccionado de forma predeterminada.
   - **Profundo**. El analizador heurístico realiza más operaciones encontradas en archivos ejecutables. La probabilidad de detección de amenazas en este modo es mayor. El análisis consume más recursos del sistema, lleva más tiempo y puede causar un número más alto de falsas alarmas.

     El control deslizante está disponible si la casilla **Usar el analizador heurístico** está seleccionada.
4. En la sección **Integración con otros componentes**, configure las siguientes opciones:
   - Seleccione o desactive la casilla de verificación **Aplicar la Zona de confianza**.

     Esta casilla de verificación habilita y deshabilita el uso de la Zona de confianza para una tarea.

Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security agrega operaciones del archivo de procesos de confianza a las exclusiones de análisis configuradas en la tarea.

Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security ignora las operaciones del archivo de procesos de confianza al formar el alcance de la protección para la tarea.

De forma predeterminada, la casilla está activada.

Haga clic en el vínculo **Zona de confianza** para abrir la configuración de la Zona de confianza.

- Seleccione o desactive la casilla de verificación **Usar KSN para protección**.

  Esta casilla de verificación habilita o deshabilita el uso de servicios de KSN.

  Si se selecciona la casilla, la aplicación utiliza los datos de Kaspersky Security Network para asegurarse de que la aplicación responda con mayor rapidez a amenazas nuevas y para reducir la posibilidad de falsos positivos.

  Si la casilla de verificación está desactivada, la tarea no usa los servicios de KSN.

  De forma predeterminada, la casilla está activada.

  La casilla de verificación **Enviar datos sobre archivos analizados** debe estar seleccionada en la configuración de la tarea Uso de KSN.

- Seleccione o desactive la casilla de verificación **Bloquear acceso a recursos compartidos en la red para los hosts que muestran actividad maliciosa**.

5. Haga clic en **Aceptar**.

Se aplicará la configuración reciente.

Configuración de las opciones de programación de inicio de tareas

Puede configurar la programación de inicio de las tareas personalizadas y del sistema local en la Consola de la aplicación. No puede configurar la programación de inicio de tareas de grupo.

► *Para configurar las opciones de programación de inicio de tareas:*

1. Abra el menú contextual de la tarea para la que desea configurar la programación del inicio.
2. Seleccione **Propiedades**.

   Se abre la ventana **Configuración de tareas**.
3. En la ventana que se abre, en la pestaña **Programación**, seleccione la casilla de verificación **Ejecutar según programación**.
4. Configure los valores de programación de acuerdo con sus requisitos. Para ello, realice las siguientes acciones:

   a. En **Frecuencia**, seleccione uno de los siguientes valores:

   - **Horaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de horas; especifique el número de horas en el campo **Cada <número> hora(s)**.
   - **Diaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de días; especifique el número de horas en el campo **Cada <número> día(s)**.

- **Semanal**, si desea que la tarea se ejecute con intervalos durante un número especificado de semanas; especifique el número de horas en el campo **Cada <número> semana(s)**. Especifique los días de la semana durante los cuales la tarea se iniciará (de manera predeterminada, las tareas se ejecutan los lunes).
- **Al inicio de la aplicación**, si desea que la tarea se ejecute cada vez que se inicia Kaspersky Embedded Systems Security.
- **Tras la actualización de bases de datos de la aplicación**, si desea que la tarea se ejecute después de cada actualización de bases de datos de la aplicación.

b. Especifique la hora del primer inicio de la tarea en el campo **Hora de inicio**.

c. En el campo **Fecha de inicio**, especifique la fecha desde la que se aplicará la programación.

Después de especificar la frecuencia de inicio de la tarea, la hora del primer inicio de esta y la fecha desde la que se aplicará la programación, la información sobre la hora calculada para el próximo inicio de la tarea se mostrará en la parte superior de la ventana en el campo **Próximo inicio**. La información actualizada sobre la hora estimada del próximo inicio de la tarea se mostrará cada vez que abra la ventana **Configuración de tareas** de la pestaña **Programación**. El campo **Bloqueado por directiva** se muestra en el campo **Próximo inicio** si las tareas de inicio del sistema en una programación están configuradas en las opciones de la directiva de Kaspersky Security Center.

5. Use la pestaña **Avanzado** para configurar las siguientes opciones de programación de acuerdo con sus requisitos.
   - En la sección **Configuración de detención de la tarea**:
     a. Seleccione la casilla de verificación **Duración** y escriba el número requerido de horas y minutos en los campos a la derecha para especificar la duración máxima de la ejecución de la tarea.
     b. Seleccione la casilla de verificación **Pausar de** y escriba los valores de inicio y de finalización del intervalo de tiempo en los campos a la derecha para especificar el intervalo de tiempo inferior a 24 horas durante el cual la ejecución de la tarea se pausará.
   - En la sección **Configuración avanzada**:
     a. Seleccione la casilla de verificación **Fin de la programación** y especifique la fecha desde la cual la programación dejará de funcionar.
     b. Seleccione la casilla de verificación **Ejecutar tareas omitidas** para habilitar el inicio de las tareas omitidas.
     c. Seleccione la casilla de verificación **Aleatorizar el inicio de la tarea usando un margen de** y especifique el valor en minutos.
6. Haga clic en **Aceptar**.

Se guarda la configuración de inicio de la tarea.

Creación del alcance de la protección

Esta sección proporciona instrucciones sobre la creación y la administración de un alcance de la protección en la tarea Protección de archivos en tiempo real.

En esta sección

Creación del alcance de la protección

El procedimiento para crear el área de la tarea de protección de archivos en tiempo real depende del modo de visualización de los recursos de archivos en red (consulte la sección "Acerca del alcance de la protección de la tarea y la configuración de seguridad" en la página 231). Puede configurar el modo de visualización de los recursos de archivos en red como un árbol o como una lista (configurado de manera predeterminada).

Para aplicar los nuevos ajustes del alcance de la protección a la tarea, se debe reanudar la tarea Protección de archivos en tiempo real.

► *Para crear un alcance de la protección con el árbol de recursos de archivos en red:*

1. Abra la ventana **Configuración del área de protección** (consulte la sección "Cómo abrir la configuración del alcance de la Protección de archivos en tiempo real" en la página 254).
2. En la sección izquierda de la ventana, abra el árbol de recursos de archivos en red para ver todos los nodos y nodos secundarios.
3. Haga lo siguiente:
   - Para excluir nodos individuales del alcance de la protección, desactive las casillas de verificación al lado de los nombres de estos nodos.
   - Para incluir nodos individuales al alcance de la protección, desactive la casilla de verificación **Mi equipo** y realice lo siguiente:
     - Si desea incluir todas las unidades de un tipo en el alcance de la protección, seleccione la casilla opuesta al nombre del tipo de disco requerido (por ejemplo, para agregar todas las unidades extraíbles del equipo, seleccione la casilla **Unidades extraíbles**).
     - Si desea incluir un disco individual de un determinado tipo en el alcance de la protección, expanda el nodo que contiene la lista de unidades de este tipo y seleccione la casilla junto al nombre de la unidad requerida. Por ejemplo, para seleccionar la unidad extraíble F:, expanda el nodo **Unidades extraíbles** y seleccione la casilla correspondiente al disco **F:**.
     - Si desea incluir solamente una carpeta o un archivo de la unidad, seleccione la casilla de verificación ubicada al lado del nombre de esa carpeta o de ese archivo.
4. Haga clic en el botón **Guardar**.

Se cerrará la ventana Configuración del alcance de la protección. Se guardaron las opciones configuradas recientemente.

► *Para crear un alcance de la protección utilizando la lista de recursos de archivos en red:*

1. Abra la ventana **Configuración del área de protección** (consulte la sección "Cómo abrir la configuración del alcance de la Protección de archivos en tiempo real" en la página 254).
2. Para incluir nodos individuales al alcance de la protección, desactive la casilla de verificación **Mi equipo** y realice lo siguiente:
   a. Abra el menú contextual del alcance de la protección haciendo clic en él con el botón derecho del mouse.
   b. En el menú contextual del botón, seleccione **Agregar área de protección**.
   c. En la ventana **Agregar área de protección**, seleccione un tipo de objeto para agregarlo a un alcance de la protección:
      - **Área predefinida** para incluir una de las áreas predefinidas en el alcance de la protección en el equipo. A continuación, en la lista desplegable, seleccione un alcance de la protección necesaria.
      - **Disco, carpeta o ubicación de red** para incluir una unidad individual, carpeta o un objeto de red en un alcance de la protección. A continuación, seleccione un área necesaria con un clic en el botón **Examinar**.
      - **Archivo** para incluir un archivo particular en el alcance de la protección. A continuación, seleccione un área necesaria con un clic en el botón **Examinar**.

      No puede agregar un objeto al alcance de la protección si ya se agregó como una exclusión de un alcance de la protección.
3. Para excluir nodos individuales del alcance de la protección, desactive las casillas al lado de los nombres de estos nodos o siga estos pasos:
   a. Abra el menú contextual del alcance de la protección haciendo clic en él con el botón derecho del mouse.
   b. En el menú contextual, seleccione la opción **Agregar exclusión**.
   c. En la ventana **Agregar exclusión**, seleccione un tipo de objeto que desee agregar como una exclusión del alcance de la protección siguiendo la lógica del objeto agregado a un procedimiento de alcance de la protección.
4. Para modificar el alcance de la protección o una exclusión agregada, seleccione la opción **Editar área** en el menú contextual del alcance de la protección necesaria.
5. Para ocultar el alcance de la protección agregada anteriormente o una exclusión en la lista de recursos de archivos en red, seleccione la opción **Eliminar de la lista** en el menú contextual del alcance de la protección necesaria.

   El alcance de la protección se excluye del alcance de la tarea de Protección de archivos en tiempo real al ser eliminada de la lista de recursos de archivos en red.
6. Haga clic en el botón **Guardar**.

Se cerrará la ventana Configuración del alcance de la protección. Se guardaron las opciones configuradas recientemente.

La tarea de *Protección de archivos en tiempo real* puede iniciarse solo si al menos uno de los nodos de recursos de archivos del equipo se incluye en un alcance de la protección.

Si se especifica un alcance de la protección compleja, por ejemplo, si se especifican valores de seguridad diferentes para la configuración de varios nodos en el árbol de recursos de archivos del equipo, puede provocar cierta ralentización en el análisis de objetos al acceder a ellos.

Creación del área virtual de protección

Se puede ampliar el área del análisis o protección si se agregan unidades virtuales, carpetas o archivos individuales solo si el área del análisis o protección se presenta como un árbol de recursos de archivo (consulte la sección “Configuración del modo de visualización para recursos de archivos en red”, en la página 427).

► *Para agregar una unidad virtual al alcance de la protección:*

1. Abra la ventana **Configuración del área de protección** (consulte la sección "Cómo abrir la configuración del alcance de la Protección de archivos en tiempo real" en la página 254).
2. Abra la lista desplegable en la ventana del sector izquierdo superior y seleccione **Vista de árbol**.
3. Abra el menú contextual de las **Unidades virtuales**.
4. Seleccione la opción **Agregar unidad virtual.**
5. En la lista de nombres disponibles, seleccione un nombre para la unidad virtual que se está creando.
6. Active la casilla junto a la unidad agregada para incluir la unidad en el alcance de la protección.
7. En la ventana **Configuración del área de protección**, haga clic en el botón **Guardar**.

Se guardaron las opciones configuradas recientemente.

► *Para agregar un archivo o carpeta virtual al alcance de la protección:*

1. Abra la ventana **Configuración del área de protección** (consulte la sección "Cómo abrir la configuración del alcance de la Protección de archivos en tiempo real" en la página 254).
2. Abra la lista desplegable en la ventana del sector izquierdo superior y seleccione **Vista de árbol**.
3. Abra el menú contextual de la unidad virtual a la cual desea agregar una carpeta o un archivo y seleccione una de las opciones siguientes:
   - **Agregar carpeta virtual** si desea agregar una carpeta virtual al alcance de la protección.
   - **Agregar archivo virtual** si desea agregar un archivo virtual al alcance de la protección.
4. En el campo de entrada, especifique el nombre de la carpeta o el archivo.
5. En la línea que contiene el nombre de la carpeta o el archivo creado, seleccione la casilla de verificación para incluir la carpeta o el archivo en el alcance de la protección.
6. En la ventana **Configuración del área de protección**, haga clic en el botón **Guardar**.

Se guarda la configuración de la tarea modificada.

Configuración manual de las opciones de seguridad

De manera predeterminada, las tareas de Protección del equipo en tiempo real utilizan la configuración de seguridad para todo el alcance de la protección. Estos ajustes corresponden a los del nivel de seguridad predefinido **Recomendado** (consulte la sección “Niveles de seguridad predefinidos”, en la página 233).

Los valores predeterminados de la configuración de seguridad se pueden modificar configurándolos como valores comunes para todo el alcance de la protección, o como valores diferentes para los diversos elementos de la lista de recursos de archivos del equipo o nodos del árbol.

Al trabajar con el árbol de recursos de archivos del servidor, las opciones de seguridad que se configuran para el nodo principal seleccionado se aplican automáticamente a todos los nodos secundarios. La configuración de seguridad del nodo principal no se aplica a nodos secundarios que se configuran por separado.

► *Para configurar las opciones de seguridad manualmente:*

1. Abra la ventana **Configuración del área de protección** (consulte la sección "Cómo abrir la configuración del alcance de la Protección de archivos en tiempo real" en la página 254).
2. En la sección de la ventana izquierda, seleccione el nodo para configurar las opciones de seguridad.

   Puede aplicarse una plantilla predefinida que contiene una configuración de seguridad (consulte la sección “Acerca de las plantillas de configuración de seguridad”, en la página 155) para un nodo o elemento seleccionado en el alcance de la protección.

3. Configure los valores de seguridad requeridos del nodo o elemento seleccionado de acuerdo con sus requisitos:
   - **General** (consulte la sección “**Configuración general de las opciones de tareas**”, en la página 262)
   - **Acciones** (consulte la sección “**Configuración de acciones**”, en la página 265)
   - **Rendimiento** (consulte la sección “**Configuración de rendimiento**”, en la página 267)
4. En la ventana **Configuración del área de protección**, haga clic en el botón **Guardar**.

Se guarda la nueva configuración del alcance de la protección.

En esta sección

Configuración de las opciones generales de tareas

► *Para configurar las opciones de seguridad generales de la tarea Protección de archivos en tiempo real:*

1. Abra la ventana **Configuración del área de protección** (consulte la sección "Cómo abrir la configuración del alcance de la Protección de archivos en tiempo real" en la página 254).
2. Seleccione la pestaña **General**.

3. En la sección **Protección de objetos**, especifique los objetos que desea incluir en el alcance de la protección:

   - **Todos los objetos**

     Kaspersky Embedded Systems Security analiza todos los objetos.

   - **Objetos analizados según su formato**

     Kaspersky Embedded Systems Security solo analiza los objetos infectables según el formato del archivo.

     Kaspersky Lab compila la lista de formatos. Se incluye en las bases de datos de Kaspersky Embedded Systems Security.

   - **Objetos analizados según la lista de extensiones de la base de datos antivirus**

     Kaspersky Embedded Systems Security solo analiza los objetos infectables según la extensión del archivo.

     Kaspersky Lab compila la lista de extensiones. Se incluye en las bases de datos de Kaspersky Embedded Systems Security.

   - **Objetos analizados según la lista de extensiones especificada**

     Kaspersky Embedded Systems Security analiza los archivos según su extensión. La lista de extensiones de archivos se puede personalizar manualmente en la ventana **Lista de extensiones**, que se puede abrir con un clic en el botón **Editar**.

   - **Analizar sectores de inicio del disco y MBR**

     Habilita la protección de los sectores de inicio y los registros de inicio maestros.

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los sectores de inicio y los registros de inicio maestro en los discos duros y las unidades extraíbles del equipo.

     De forma predeterminada, la casilla está activada.

   - **Analizar secuencias alternativas de NTFS**

     Análisis de flujos de archivos y carpetas alternativos en las unidades del sistema de archivos NTFS.

     Si se selecciona la casilla de verificación, la aplicación analiza un objeto probablemente infectado y todos los flujos NTFS asociados con ese objeto.

     Si se cancela la selección de la casilla de verificación, la aplicación solo analiza el objeto que se detectó y se consideró como probablemente infectado.

     De forma predeterminada, la casilla está activada.

4. En la sección **Rendimiento**, seleccione o cancele la selección de la casilla de verificación **Proteger solo los archivos nuevos y modificados**.

   Esta casilla de verificación activa y desactiva el análisis y la protección de archivos que Kaspersky Embedded Systems Security reconoció como nuevos o modificados desde el último análisis.

   Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza y protege solo los archivos que reconoció como nuevos o modificados desde el último análisis.

   Si se cancela la selección de la casilla de verificación, puede seleccionar si desea analizar y proteger solo archivos nuevos o todos los archivos, más allá de su estado de

modificación.

De forma predeterminada, la casilla está activada para el nivel de seguridad **Máximo Rendimiento**. Si se configuran los niveles de seguridad **Máxima Protección** o **Recomendado**, la casilla de verificación se desactiva.

Para cambiar entre opciones disponibles cuando la casilla está desactivada, haga clic en el vínculo **Todos** / **Solo nuevos** para cada uno de los tipos de objeto compuestos.

5. En la sección **Protección de objetos compuestos**, especifique los objetos compuestos que desea incluir en el alcance de la protección:

- **Todos/Solo nuevos archivos comprimidos**

  Análisis de archivos ZIP, CAB, RAR, ARJ y otros formatos de archivos.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los archivos comprimidos.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos comprimidos durante el análisis.

  El valor predeterminado depende del nivel de protección seleccionado.

- **Todos/Solo nuevos archivos SFX**

  Análisis de archivos autoextraíbles.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza archivos SFX.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos SFX durante el análisis.

  El valor predeterminado depende del nivel de protección seleccionado.

  Esta opción se encuentra activa cuando la casilla de verificación **Archivos comprimidos** está desactivada.

- **Todos/Solo nuevas bases de datos de correo electrónico**

  Análisis de archivos de bases de datos de correo de Microsoft Outlook y Microsoft Outlook Express.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza todos los archivos de la base de datos de correo.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos de la base de datos de correo durante el análisis.

  El valor predeterminado depende del nivel de seguridad seleccionado.

- **Todos/Solo nuevos objetos empaquetados**

  Análisis de archivos ejecutables empaquetados mediante compresores de código binario, tales como UPX o ASPack.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los archivos ejecutables empaquetados por empaquetadores.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos ejecutables empaquetados por empaquetadores durante el análisis.

El valor predeterminado depende del nivel de protección seleccionado.

- **Todos/Solo nuevo correo electrónico simple**

  Análisis de archivos de formatos de correo, tales como mensajes de Microsoft Outlook y Microsoft Outlook Express.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los archivos con formato de correo.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos con formato de correo durante el análisis.

  El valor predeterminado depende del nivel de seguridad seleccionado.

- **Todos/Solo nuevos objetos OLE incorporados**

  Análisis de objetos integrados en archivos (por ejemplo, macros de Microsoft Word o archivos adjuntos del mensaje de correo electrónico).

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los objetos integrados en archivos.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los objetos integrados en archivos durante el análisis.

  El valor predeterminado depende del nivel de protección seleccionado.

6. Haga clic en **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de acciones

► *Para configurar las acciones en objetos infectados y otros objetos detectados para la tarea de Protección de archivos en tiempo real:*

1. Abra la ventana **Configuración del área de protección** (consulte la sección "Cómo abrir la configuración del alcance de la Protección de archivos en tiempo real" en la página 254).
2. Seleccione la pestaña **Acciones**.
3. Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:

   - **Solo notificar**.

     Cuando se selecciona este modo, Kaspersky Embedded Systems Security no bloquea el acceso a los objetos infectados y a otros objetos detectados ni realiza ninguna acción relacionada con ellos. Se registra el siguiente evento en el registro de tareas: *Objeto no desinfectado. Motivo: No se tomó ninguna acción para neutralizar el objeto detectado debido a la configuración definida por el usuario.* El evento especifica toda la información disponible sobre el objeto detectado.

     El modo **Solo notificar** debe configurarse por separado para cada área de protección o análisis. Este modo no se usa de forma predeterminada en ninguno de los niveles de seguridad. Si selecciona este modo, Kaspersky Embedded Systems Security cambia automáticamente el nivel de seguridad a **Personalizado**.

   - **Bloquear acceso**.

     Cuando se selecciona esta opción, Kaspersky Embedded Systems Security bloquea el acceso al objeto detectado o probablemente infectado. Puede seleccionar una acción

adicional sobre los objetos bloqueados en la lista desplegable.

- **Realizar acción adicional**.

  Seleccione la acción en la lista desplegable:

  - **Desinfectar**.
  - **Desinfectar. Desinfectar; si falla la desinfección, eliminar**.
  - **Eliminar**.
  - **Recomendado**.

4. Seleccione la acción a realizar en los objetos probablemente infectados:

   - **Solo notificar**.

     Cuando se selecciona este modo, Kaspersky Embedded Systems Security no bloquea el acceso a los objetos infectados y a otros objetos detectados ni realiza ninguna acción relacionada con ellos. Se registra el siguiente evento en el registro de tareas: *Objeto no desinfectado. Motivo: No se tomó ninguna acción para neutralizar el objeto detectado debido a la configuración definida por el usuario.* El evento especifica toda la información disponible sobre el objeto detectado.

     El modo **Solo notificar** debe configurarse por separado para cada área de protección o análisis. Este modo no se usa de forma predeterminada en ninguno de los niveles de seguridad. Si selecciona este modo, Kaspersky Embedded Systems Security cambia automáticamente el nivel de seguridad a **Personalizado**.

   - **Bloquear acceso**.

     Cuando se selecciona esta opción, Kaspersky Embedded Systems Security bloquea el acceso al objeto detectado o probablemente infectado. Puede seleccionar una acción adicional sobre los objetos bloqueados en la lista desplegable.

   - **Realizar acción adicional**.

     Seleccione la acción en la lista desplegable:

     - **Poner en cuarentena**.
     - **Eliminar**.
     - **Recomendado**.

5. Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:

   a. Borre o seleccione la casilla de verificación **Realizar acciones según el tipo de objeto detectado**.

      Si se selecciona la casilla, puede configurar independientemente la acción principal y secundaria para cada tipo de objeto detectado haciendo clic en el botón **Configurar** ubicado junto a la casilla de verificación. En ese momento, Kaspersky Embedded Systems Security no permitirá abrir o ejecutar un objeto infectado, independientemente de su elección.

      Si la casilla de verificación no está seleccionada, Kaspersky Embedded Systems Security realiza las acciones seleccionadas en las secciones **Acción que se realizará con los objetos infectados y otros objetos** y **Acción que se realizará con los objetos probablemente infectados** para los tipos de objetos correspondientes.

      De forma predeterminada, la casilla está desactivada.

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

   c. En la ventana que se abre, seleccione la acción primaria y secundaria (en caso de que falle la

primaria) para cada tipo de objeto detectado.

d. Haga clic en **Aceptar**.

6. Seleccione la acción a realizar en archivos compuestos no modificables: seleccione o borre la casilla de verificación **Si se detecta un objeto integrado infectado, eliminar todo el archivo compuesto si la aplicación no puede modificarlo**.

   Esta casilla habilita o deshabilita la eliminación forzada del archivo compuesto principal cuando se detecta un objeto secundario malicioso, probablemente infectado u otro objeto secundario integrado.

   Si se selecciona la casilla de verificación y se configura la tarea para eliminar los objetos infectados y probablemente infectados. Kaspersky Embedded Systems Security elimina de manera forzada todo el objeto compuesto principal cuando se detecta un objeto malicioso u otro objeto integrado. La eliminación forzada de un archivo principal junto con todo su contenido sucede si la aplicación no puede eliminar únicamente el objeto secundario detectado (por ejemplo, si el objeto principal es inmodificable).

   Si se desactiva esta casilla y la tarea se configura para eliminar objetos infectados y probablemente infectados, Kaspersky Embedded Systems Security no realiza la acción seleccionada si el objeto principal es inmodificable.

7. Haga clic en **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de rendimiento

► *Para configurar el rendimiento para la tarea Protección de archivos en tiempo real:*

1. Abra la ventana **Configuración del área de protección** (consulte la sección "Cómo abrir la configuración del alcance de la Protección de archivos en tiempo real" en la página 254).
2. Seleccione la pestaña **Rendimiento**.
3. En la sección **Exclusiones**:
   - Borre o seleccione la casilla de verificación **Excluir archivos**.

     Excluir archivos del análisis por nombre de archivo o máscara de nombre de archivo.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos especificados durante el análisis.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza todos los objetos.

     De forma predeterminada, la casilla está desactivada.

   - Borre o seleccione la casilla de verificación **No detectar**.

     Los objetos se excluyen del análisis por el nombre o la máscara del nombre del objeto detectable. La lista de nombres de objetos detectables está disponible en el sitio web de la Enciclopedia de Virus https://encyclopedia.kaspersky.com/knowledge/classification/

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos especificados detectables durante el análisis.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security detecta todos los objetos especificados en la aplicación de forma predeterminada.

De forma predeterminada, la casilla está desactivada.

- Haga clic en el botón **Editar** en cada para parámetro agregar exclusiones.

4. En la sección **Configuración avanzada**:

- **Detener el análisis si demora más de (seg.)**

  Limita la duración del análisis de objetos. El valor predeterminado es 60 segundos.

  Si la casilla está desactivada, la duración del análisis se limita al valor especificado.

  Si la casilla está desactivada, la duración del análisis es ilimitada.

  De forma predeterminada, la casilla está activada para el nivel de seguridad **Máximo Rendimiento**.

- **Omitir objetos compuestos de más de (MB)**

  Excluye del análisis objetos más grandes que el tamaño especificado.

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos compuestos cuyo tamaño supera el límite especificado durante el análisis antivirus.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza los objetos compuestos de cualquier tamaño.

  De forma predeterminada, la casilla está activada para el nivel de seguridad **Máximo Rendimiento**.

- **Usar la tecnología iSwift**

  iSwift compara el identificador NTFS del archivo, que está almacenado en una base de datos, con un identificador actual. El análisis se realiza solo para archivos cuyos identificadores han cambiado (archivos nuevos y archivos modificados desde el último análisis de objetos del sistema NTFS).

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security solo analiza los archivos nuevos o modificados desde el último análisis de objetos del sistema NTFS.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza los objetos del sistema del archivo NTFS sin considerar la fecha de creación o modificación del archivo, excepto los archivos de carpetas de red.

  De forma predeterminada, la casilla está activada.

- **Usar la tecnología iChecker**

  iChecker calcula y recuerda las sumas de control de los archivos analizados. Si un objeto se modifica, la suma de control cambia. La aplicación compara todas las sumas de control durante la tarea de análisis, y analiza solo los archivos nuevos y modificados desde el último análisis.

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza solo los archivos nuevos y modificados.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza los archivos sin considerar la fecha de creación o modificación del archivo.

  De forma predeterminada, la casilla está activada.

Estadísticas de la tarea de Protección de archivos en tiempo real

Mientras se ejecuta la tarea de Protección de archivos en tiempo real, puede ver información detallada en tiempo real sobre la cantidad de objetos procesados por Kaspersky Embedded Systems Security desde que la tarea se inició hasta el momento actual.

► *Para ver las estadísticas de una tarea de Protección de archivos en tiempo real, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Protección de archivos en tiempo real**.

   Las estadísticas de la tarea se muestran en la sección **Estadísticas** del panel de detalles del nodo seleccionado.

Se puede ver la información sobre los objetos procesados por Kaspersky Embedded Systems Security desde que se inició hasta el momento actual (consulte la tabla a continuación):

Tabla 43. Estadísticas de la tarea de Protección de archivos en tiempo real

Campo	Descripción
Detectado	Número de objetos detectados por Kaspersky Embedded Systems Security. Por ejemplo, si Kaspersky Embedded Systems Security detecta un programa de malware en cinco archivos, el valor de este campo aumenta en uno.
Objetos infectados y otros objetos detectados	La cantidad de objetos que Kaspersky Embedded Systems Security encontró y clasificó como infectados, o la cantidad encontrada de archivos de software legítimos que los intrusos pueden usar para dañar su equipo o sus datos personales.
Objetos probablemente infectados detectados	Cantidad de objetos probablemente infectados encontrados por Kaspersky Embedded Systems Security.
Objetos no desinfectados	Cantidad de objetos que Kaspersky Embedded Systems Security no desinfectó debido a los siguientes motivos: • El tipo de objeto detectado no se puede desinfectar. • Se produjo un error durante la desinfección.
Objetos que no se pasaron a Cuarentena	Cantidad de objetos que Kaspersky Embedded Systems Security intentó poner en cuarentena pero no pudo, por ejemplo, debido a espacio insuficiente en el disco.
Objetos no eliminados	Cantidad de objetos que Kaspersky Embedded Systems Security intentó eliminar, pero no pudo hacerlo debido a que, por ejemplo, el acceso al objeto estaba bloqueado por otra aplicación.
Objetos no analizados	Cantidad de objetos en el alcance de la protección que Kaspersky Embedded Systems Security no pudo analizar debido a que, por ejemplo, el acceso al objeto estaba bloqueado por otra aplicación.
Objetos sin copia de seguridad	Una cantidad de objetos cuyas copias Kaspersky Embedded Systems Security intentó guardar en Copia de seguridad, pero no pudo hacerlo; por ejemplo, debido a espacio insuficiente en el disco.
Errores de procesamiento	Cantidad de objetos en los que se produjo un error durante su procesamiento.

Campo	Descripción
Objetos desinfectados	Número de objetos desinfectados por Kaspersky Embedded Systems Security.
Pasados a Cuarentena	Número de objetos pasados a Cuarentena por Kaspersky Embedded Systems Security.
Objetos pasados a Copia de seguridad	La cantidad de copias de objetos que Kaspersky Embedded Systems Security guardó en Copia de seguridad.
Objetos eliminados	Número de objetos eliminados por Kaspersky Embedded Systems Security.
Objetos protegidos con contraseña	Cantidad de objetos (por ejemplo, archivos) que Kaspersky Embedded Systems Security omitió porque estaban protegidos por contraseña.
Objetos dañados	Cantidad de objetos omitidos por Kaspersky Embedded Systems Security debido a que el formato estaba dañado.
Objetos procesados	Cantidad total de objetos que procesó Kaspersky Embedded Systems Security.

Puede ver las estadísticas de la tarea de Protección de archivos en tiempo real en el registro de tareas si hace clic en **Abrir el registro de tareas** en la sección **Administración** del panel de detalles.

Si el valor del campo **Eventos en total** en la ventana del registro de tareas de Protección en tiempo real supera 0, se recomienda procesar los eventos que aparecen en el registro de tareas en la pestaña **Eventos** manualmente.

Uso de KSN

Esta sección contiene información acerca de la tarea de Uso de KSN y cómo configurarla.

En este capítulo

Acerca de la tarea Uso de KSN

Kaspersky Security Network (también denominado “KSN”) es una infraestructura de servicios en línea que proporciona acceso a la base de conocimientos operativa de Kaspersky Lab sobre la reputación de archivos, recursos web y programas. Kaspersky Security Network permite que Kaspersky Embedded Systems Security reaccione rápidamente ante amenazas nuevas, mejora el rendimiento de varios componentes de protección y reduce la posibilidad de falsos positivos.

Para iniciar la tarea Uso de KSN, debe aceptar la Declaración de Kaspersky Security Network.

La información recibida por Kaspersky Embedded Systems Security de Kaspersky Security Network solo pertenece a la reputación de los programas.

La participación en KSN permite a Kaspersky Lab recibir información en tiempo real sobre tipos y fuentes de amenazas nuevas, desarrollar modos de neutralizarlas y reducir el número de falsos positivos en los componentes de la aplicación.

La información más detallada sobre la transferencia, el procesamiento, el almacenamiento y la destrucción de información sobre uso de aplicaciones está disponible en la ventana **Manejo de datos** de la tarea Uso de KSN, y en la Política de privacidad en el sitio web de Kaspersky Lab.

La participación en Kaspersky Security Network es voluntaria. La decisión en cuanto a la participación en Kaspersky Security Network se toma después de la instalación de Kaspersky Embedded Systems Security. Puede cambiar de opinión sobre la participación en Kaspersky Security Network en cualquier momento.

Kaspersky Security Network puede utilizarse en las siguientes tareas de Kaspersky Embedded Systems Security:

- Protección de archivos en tiempo real.
- Análisis a pedido.
- Control de inicio de aplicaciones.

Kaspersky Security Network Privada

Consulte detalles sobre la forma de configurar Kaspersky Security Network Privada (de aquí en más, “KSN Privada”) en la *Ayuda de Kaspersky Security Center*.

Si utiliza KSN Privada en el equipo protegido, vaya a la ventana **Manejo de datos** (consulte la sección “Configuración de Manejo de datos mediante el complemento de administración” en la página 276) de la tarea Uso de KSN que puede leer en la Declaración de KSN y habilite la tarea seleccionando la casilla **Acepto la Declaración de Kaspersky Private Security Network**. Al aceptar los términos, acepta enviar todos los tipos de datos mencionados en la Declaración de KSN (solicitudes de seguridad, datos estadísticos) a servicios de KSN.

Después de aceptar los términos de KSN Privada, las casillas de verificación que configuran el uso de KSN global no están disponibles.

Si deshabilita KSN Privada cuando se está ejecutando la tarea Uso de KSN, se produce el error *Infracción de la licencia* y la tarea se detiene. Para seguir protegiendo el equipo, debe aceptar la Declaración de KSN en la ventana **Manejo de datos** y reiniciar la tarea.

Cancelación de la aceptación de la Declaración de KSN

Puede cancelar la aceptación y detener todo intercambio de datos con Kaspersky Security Network en cualquier momento. Las siguientes acciones se consideran como una cancelación completa o parcial de la Declaración de KSN:

- Si se desactiva la casilla de verificación **Enviar datos sobre archivos analizados**: la aplicación deja de enviar sumas de control de archivos analizados al servicio de KSN.
- Si se desactiva la casilla de verificación **Enviar estadísticas de Kaspersky Security Network**: la aplicación deja de procesar datos con estadísticas de KSN adicionales.
- Si se desactiva la casilla de verificación **Acepto los términos de la Declaración de Kaspersky Security Network**: la aplicación detiene todo el procesamiento de datos relacionados con KSN y se detiene la tarea Uso de KSN.
- Si se desinstala el componente Uso de KSN: se detiene todo el procesamiento de datos relacionado con KSN.
- Si se desinstala Kaspersky Embedded Systems Security: se detiene todo el procesamiento de datos relacionado con KSN.

Configuración de tarea predeterminada de Uso de KSN

Puede cambiar la configuración predeterminada de la tarea Uso de KSN (consulte la siguiente tabla).

Tabla 44. Configuración de tarea predeterminada de Uso de KSN

Configuración	Valor predeterminado	Descripción
Acción para realizar con los objetos no confiables según KSN	Eliminar	Puede especificar acciones que Kaspersky Embedded Systems Security tomará sobre los objetos identificados por KSN como dudosos.
Transferencia de datos	Se calcula la suma de control del archivo (hash MD5) para los archivos que no superan 2 MB de tamaño.	Puede especificar el tamaño máximo de archivos para los cuales se calcula una suma de control con el algoritmo MD5 para la entrega a KSN. Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security calcula el hash MD5 para los archivos de cualquier tamaño.
Programación de inicio de tareas	La primera ejecución no está programada.	Puede iniciar la tarea manualmente o configurar un inicio programado.
Usar Kaspersky Security Center como KSN Proxy	Seleccionada	De forma predeterminada, los datos se envían a KSN mediante Kaspersky Security Center. Puede cambiar esta configuración solo mediante el Complemento de administración.
Acepto los términos de la Declaración de Kaspersky Security Network	Desactivada	Si se selecciona, acepta la participación en KSN después de la instalación. Puede cambiar su decisión en cualquier momento.
Enviar estadísticas de Kaspersky Security Network	Seleccionado (se aplica solo si se aceptó la Declaración de KSN)	Si se aceptó la Declaración de KSN, se enviarán automáticamente las estadísticas de KSN a menos que desactive la casilla de verificación.
Enviar datos sobre archivos analizados	Seleccionado (se aplica solo si se aceptó la Declaración de KSN)	Si se aceptó la Declaración de KSN, se envían los datos sobre los archivos analizados desde el inicio de la tarea. Puede desactivar la casilla de verificación en cualquier momento.
Enviar datos sobre URL analizadas	Seleccionado (se aplica solo si se aceptó la Declaración de KSN)	Si acepta la Declaración de KSN, la aplicación envía a Kaspersky Lab la información sobre las direcciones URL a las que se accedió.
Acepte los términos de la Declaración de Kaspersky Managed Protection	Desactivada	Puede habilitar o deshabilitar el servicio KMP. El servicio está disponible solo si se firmó el acuerdo adicional durante el proceso de compra de la aplicación.

Gestión del Uso de KSN a través del Complemento de administración

En esta sección, aprenda cómo configurar la tarea Uso de KSN y Manejo de datos mediante el Complemento de administración.

En esta sección

Configuración de la tarea de Uso de KSN mediante el Complemento de administración

► *Para configurar la tarea Uso de KSN, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.
4. En la sección **Protección del equipo en tiempo real**, haga clic en el botón **Configurar** en el bloque **Uso de KSN**.

   Se abre la ventana **Uso de KSN**.

5. En la pestaña **General**, configure la siguiente configuración de tarea:

   - En la sección **Acción para realizar con los objetos no confiables según KSN**, especifique la acción que Kaspersky Embedded Systems Security debe realizar si detecta un objeto identificado por KSN como dudoso:

     - **Eliminar**

       Kaspersky Embedded Systems Security elimina el objeto de estado dudoso según KSN y coloca una copia en Copia de seguridad.

       De forma predeterminada, esta opción está seleccionada.

     - **Registrar información**

       Kaspersky Embedded Systems Security registra información sobre el objeto de estado dudoso según KSN en el registro de tareas. Kaspersky Embedded Systems Security no elimina el objeto dudoso.

   - En la sección **Transferencia de datos**, limite el tamaño de los archivos para los cuales se calcula la suma de control:

     - Seleccione o desactive la casilla de verificación **No calcular la suma de control antes de enviar el archivo a KSN si el tamaño del archivo es mayor a (MB)**.

       Esta casilla de verificación habilita o deshabilita el cálculo de la suma de control para archivos del tamaño especificado para la entrega de esta información al servicio KSN.

       La duración del cálculo de la suma de control depende del tamaño del archivo.

       Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security no calcula la suma de control para los archivos que superan el tamaño especificado (en MB).

       Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security calcula la suma de control para los archivos de cualquier tamaño.

       De forma predeterminada, la casilla está activada.

     - Si es necesario, en el campo a la derecha, cambie el tamaño máximo de archivos para los cuales Kaspersky Embedded Systems Security calcula la suma de control.

   - En la sección **KSN Proxy**, desactive o seleccione la casilla de verificación **Usar Kaspersky Security Center como KSN Proxy**.

     La casilla de verificación permite administrar la transferencia de datos entre los equipos protegidos y KSN.

     Si se desactiva la casilla, los datos del Servidor de administración y los equipos protegidos se envían directamente a KSN (no mediante Kaspersky Security Center). La directiva activa define qué tipo de datos pueden enviarse directamente a KSN.

     Si se selecciona la casilla, todos los datos se envían a KSN mediante Kaspersky Security Center.

     De forma predeterminada, la casilla está activada.

   Para habilitar el KSN Proxy, debe haberse aceptado la Declaración de KSN, y Kaspersky Security Center debe estar configurado correctamente. Consulte la *Ayuda de Kaspersky Security Center* para obtener más detalles.

6. De ser necesario, configure la programación de inicio de tareas en la pestaña **Administración de la tarea**.

Por ejemplo, puede iniciar la tarea según una programación y especificar la frecuencia **Al inicio de la aplicación** si desea que la tarea se ejecute automáticamente cuando se reinicia el servidor.

La aplicación iniciará automáticamente la tarea Uso de KSN según la programación.

7. Configure el Manejo de datos (consulte la sección "Configuración de Manejo de datos mediante el Complemento de administración" en la página 276) antes de iniciar la tarea.
8. Haga clic en **Aceptar**.

Se aplica la configuración modificada. La fecha y tiempo de modificación de la configuración, así como la información sobre la configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Configuración de Manejo de datos mediante el Complemento de administración

► *Para configurar los datos que procesarán los servicios de KSN y aceptar la Declaración de KSN:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.
4. En la sección **Protección del equipo en tiempo real**, haga clic en el botón **Manejo de datos** en el bloque **Uso de KSN**.

   Se abre la ventana **Manejo de datos**.
5. En la ficha **Estadísticas y servicios**, lea la declaración y seleccione la casilla de verificación **Acepto los términos de la Declaración de Kaspersky Security Network**.
6. Para aumentar el nivel de protección, se seleccionan automáticamente las siguientes casillas de verificación:
   - **Enviar datos sobre archivos analizados**.

     Si se selecciona la casilla, Kaspersky Embedded Systems Security envía la suma de control de los archivos analizados a Kaspersky Lab. La conclusión sobre la seguridad de cada archivo se basa en la reputación recibida de KSN.

     Si se desactiva la casilla, Kaspersky Embedded Systems Security no envía la suma de control de los archivos a KSN.

Tenga en cuenta que las solicitudes de reputación de archivos se podrían enviar en un modo limitado. Las limitaciones se utilizan para proteger a los servidores de reputación de Kaspersky Lab contra los ataques de DDoS. En esta situación, los parámetros de solicitudes de reputación de archivos que se envían se definen por las reglas y los métodos establecidos por los expertos de Kaspersky Lab, y no pueden ser configurados por el usuario en un equipo protegido. Las actualizaciones de estas reglas y métodos se reciben junto con las actualizaciones de la base de datos de la aplicación. Si se aplican las limitaciones, aparece el estado *Habilitado por Kaspersky Lab para proteger a los servidores de KSN contra DDoS* en las estadísticas de la tarea Uso de KSN.

De forma predeterminada, la casilla está activada.

- **Enviar estadísticas de Kaspersky Security Network.**

  Si se selecciona la casilla, Kaspersky Embedded Systems Security envía estadísticas adicionales que pueden contener datos personales. La lista de todos los datos que se envían como estadísticas de KSN se especifica en la Declaración de KSN. Los datos recibidos por Kaspersky Lab se usan para mejorar la calidad de las aplicaciones y el nivel del índice de detección de amenazas.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no envía estadísticas adicionales.

  De forma predeterminada, la casilla está activada.

Puede desactivar estas casillas de verificación y dejar de enviar datos adicionales en cualquier momento.

7. En la ficha **Kaspersky Managed Protection**, lea la declaración y seleccione la casilla de verificación **Acepto los términos de la Declaración de Kaspersky Managed Protection**.

   Si se selecciona la casilla, significa que acepta enviar estadísticas sobre la actividad del equipo protegido a los especialistas de Kaspersky Lab. Los datos recibidos se utilizan para análisis e informes las veinticuatro horas, algo que se requiere para evitar incidentes de violación de la seguridad.

   De forma predeterminada, la casilla está desactivada.

Los cambios de estado de la casilla de verificación **Acepto los términos de la Declaración de Kaspersky Managed Protection** no inician o detienen inmediatamente el procesamiento de datos. Para aplicar los cambios, debe reiniciar Kaspersky Embedded Systems Security.

Para usar el servicio KMP, debe firmar el acuerdo correspondiente y ejecutar archivos de configuración en un equipo protegido.

Para usar el servicio KMP, deben aceptarse los términos de procesamiento de datos de la Declaración de KSN en la pestaña **Estadísticas y servicios**.

8. Haga clic en **Aceptar**.

   Se guardará la configuración de procesamiento de datos.

Gestión del Uso de KSN a través de la Consola de la aplicación

En esta sección, aprenda cómo configurar la tarea Uso de KSN y Manejo de datos mediante la Consola de la aplicación.

En esta sección

Configuración de tarea Uso de KSN mediante la Consola de la aplicación

► *Para configurar la tarea Uso de KSN, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Uso de KSN**.
3. Haga clic en el vínculo **Propiedades** del panel de detalles.

   Se abre la ventana **Configuración de tareas** en la pestaña **General**.
4. Configure la tarea:
   - En la sección **Acción para realizar con los objetos no confiables según KSN**, especifique la acción que Kaspersky Embedded Systems Security debe realizar si detecta un objeto identificado por KSN como dudoso:
     - **Eliminar**

       Kaspersky Embedded Systems Security elimina el objeto de estado dudoso según KSN y coloca una copia en Copia de seguridad.

       De forma predeterminada, esta opción está seleccionada.
     - **Registrar información**

       Kaspersky Embedded Systems Security registra información sobre el objeto de estado dudoso según KSN en el registro de tareas. Kaspersky Embedded Systems Security no elimina el objeto dudoso.
   - En la sección **Transferencia de datos**, limite el tamaño de los archivos para los cuales se calcula la suma de control:
     - Seleccione o desactive la casilla de verificación **No calcular la suma de control antes de enviar el archivo a KSN si el tamaño del archivo es mayor a (MB)**.

       Esta casilla de verificación habilita o deshabilita el cálculo de la suma de control para archivos del tamaño especificado para la entrega de esta información al servicio KSN.

       La duración del cálculo de la suma de control depende del tamaño del archivo.

       Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security no calcula la suma de control para los archivos que superan el tamaño especificado

(en MB).

Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security calcula la suma de control para los archivos de cualquier tamaño.

De forma predeterminada, la casilla está activada.

- Si es necesario, en el campo a la derecha, cambie el tamaño máximo de archivos para los cuales Kaspersky Embedded Systems Security calcula la suma de control.

5. De ser necesario, configure la programación de inicio de tareas en las pestañas **Programación** y **Avanzado**. Por ejemplo, puede habilitar el inicio de la tarea según una programación y especificar la frecuencia del inicio como **Al inicio de la aplicación** si desea que la tarea se ejecute automáticamente cuando el equipo se reinicia.

   La aplicación iniciará automáticamente la tarea Uso de KSN según la programación.

6. Configure el Manejo de datos (consulte la sección “Configuración de Manejo de datos mediante la Consola de la aplicación” en la página 279) antes de iniciar la tarea.

7. Haga clic en **Aceptar**.

Se aplica la configuración modificada. La fecha y tiempo de modificación de la configuración, así como la información sobre la configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Configuración de Manejo de datos mediante la Consola de la aplicación

► *Para configurar los datos que procesarán los servicios de KSN y aceptar la Declaración de KSN:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Uso de KSN**.
3. Haga clic en el vínculo **Manejo de datos** del panel de detalles.

   Se abre la ventana **Manejo de datos**.

4. En la ficha **Estadísticas y servicios**, lea la declaración y seleccione la casilla de verificación **Acepto los términos de la Declaración de Kaspersky Security Network**.
5. Para aumentar el nivel de protección, se seleccionan automáticamente las siguientes casillas de verificación:

   - **Enviar datos sobre archivos analizados**.

     Si se selecciona la casilla, Kaspersky Embedded Systems Security envía la suma de control de los archivos analizados a Kaspersky Lab. La conclusión sobre la seguridad de cada archivo se basa en la reputación recibida de KSN.

     Si se desactiva la casilla, Kaspersky Embedded Systems Security no envía la suma de control de los archivos a KSN.

     Tenga en cuenta que las solicitudes de reputación de archivos se podrían enviar en un modo limitado. Las limitaciones se utilizan para proteger a los servidores de reputación de Kaspersky Lab contra los ataques de DDoS. En esta situación, los parámetros de solicitudes de reputación de archivos que se envían se definen por las reglas y los métodos establecidos por los expertos de Kaspersky Lab, y no pueden ser configurados

por el usuario en un equipo protegido. Las actualizaciones de estas reglas y métodos se reciben junto con las actualizaciones de la base de datos de la aplicación. Si se aplican las limitaciones, aparece el estado *Habilitado por Kaspersky Lab para proteger a los servidores de KSN contra DDoS* en las estadísticas de la tarea Uso de KSN.

De forma predeterminada, la casilla está activada.

- **Enviar estadísticas de Kaspersky Security Network.**

  Si se selecciona la casilla, Kaspersky Embedded Systems Security envía estadísticas adicionales que pueden contener datos personales. La lista de todos los datos que se envían como estadísticas de KSN se especifica en la Declaración de KSN. Los datos recibidos por Kaspersky Lab se usan para mejorar la calidad de las aplicaciones y el nivel del índice de detección de amenazas.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no envía estadísticas adicionales.

  De forma predeterminada, la casilla está activada.

Puede desactivar estas casillas de verificación y dejar de enviar datos adicionales en cualquier momento.

6. En la ficha **Kaspersky Managed Protection**, lea la declaración y seleccione la casilla de verificación **Acepto los términos de la Declaración de Kaspersky Managed Protection**.

   Si se selecciona la casilla, significa que acepta enviar estadísticas sobre la actividad del equipo protegido a los especialistas de Kaspersky Lab. Los datos recibidos se utilizan para análisis e informes las veinticuatro horas, algo que se requiere para evitar incidentes de violación de la seguridad.

   De forma predeterminada, la casilla está desactivada.

Los cambios de estado de la casilla de verificación **Acepto los términos de la Declaración de Kaspersky Managed Protection** no inician o detienen inmediatamente el procesamiento de datos. Para aplicar los cambios, debe reiniciar Kaspersky Embedded Systems Security.

Para usar el servicio KMP, debe firmar el acuerdo correspondiente y ejecutar archivos de configuración en un equipo protegido.

Para usar el servicio KMP, deben aceptarse los términos de procesamiento de datos de la Declaración de KSN en la pestaña **Estadísticas y servicios**.

7. Haga clic en **Aceptar**.

Se guardará la configuración de procesamiento de datos.

Configuración de la transferencia de datos adicional

Kaspersky Embedded Systems Security se puede configurar para enviar los siguientes datos a Kaspersky Lab:

- Sumas de control de archivos analizados (casilla de verificación **Enviar datos sobre archivos**

analizados).

- Estadísticas adicionales, incluidos datos personales (casilla de verificación **Enviar estadísticas de Kaspersky Security Network**).

> Consulte la sección “Manejo de datos locales” de este guía para acceder a información detallada sobre los datos que se envían a Kaspersky Lab.

Las casillas correspondientes se pueden seleccionar o desactivar (consulte la sección “Configuración de Manejo de datos mediante la Consola de la aplicación” en la página 279) solo si se seleccionó la casilla **Acepto los términos de la Declaración de Kaspersky Security Network**.

De forma predeterminada, Kaspersky Embedded Systems Security envía sumas de control y estadísticas adicionales después de aceptar la Declaración de KSN.

Tabla 45. Posibles estados de las casillas de verificación y condiciones correspondientes

Estado de la casilla	**Condiciones para el estado de la casilla** Enviar datos sobre archivos analizados	**Condiciones para el estado de la casilla** Enviar estadísticas de Kaspersky Security Network	**Condiciones para el estado de la casilla de verificación** Enviar datos sobre las URL analizadas	**Condiciones para del estado de la casilla de verificación** Acepto los términos de la Declaración de Kaspersky Managed Protection	**Condiciones para del estado de la casilla de verificación** Acepto los términos de la Declaración de Kaspersky Security Network
	• se envían solicitudes de reputación • la casilla es editable	• se envían estadísticas adicionales • la casilla es editable	• se envían datos sobre las URL analizadas • la casilla es editable	• se aceptan los términos de la Declaración de Kaspersky Managed Protection • la casilla es editable	• se aceptan los términos de la Declaración de Kaspersky Security Network • la casilla es editable
	• se envían solicitudes de reputación • la casilla no es editable	• se envían estadísticas adicionales • la casilla no es editable	• se envían datos sobre las URL analizadas • la casilla no es editable	• se aceptan los términos de la Declaración de Kaspersky Managed Protection • la casilla no es editable	• se aceptan los términos de la Declaración de Kaspersky Security Network • la casilla no es editable

Estado de la casilla	Condiciones para el estado de la casilla Enviar datos sobre archivos analizados	Condiciones para el estado de la casilla Enviar estadísticas de Kaspersky Security Network	Condiciones para el estado de la casilla de verificación Enviar datos sobre las URL analizadas	Condiciones para del estado de la casilla de verificación Acepto los términos de la Declaración de Kaspersky Managed Protection	Condiciones para del estado de la casilla de verificación Acepto los términos de la Declaración de Kaspersky Security Network
	• no se envían solicitudes de reputación • la casilla es editable	• no se envían estadísticas adicionales • la casilla es editable	• no se envían los datos sobre las URL analizadas • la casilla es editable	• no se aceptan los términos de la Declaración de Kaspersky Managed Protection • la casilla es editable	• no se aceptan los términos de la Declaración de Kaspersky Security Network • la casilla es editable
	• no se envían solicitudes de reputación • la casilla no es editable	• no se envían estadísticas adicionales • la casilla no es editable	• no se envían los datos sobre las URL analizadas • la casilla no es editable	• no se aceptan los términos de la Declaración de Kaspersky Managed Protection • la casilla no es editable	• no se aceptan los términos de la Declaración de Kaspersky Security Network • la casilla no es editable

Estadísticas de la tarea Uso de KSN

Mientras se está ejecutando la tarea Uso de KSN, es posible ver información detallada en tiempo real sobre el número de objetos procesados por Kaspersky Embedded Systems Security desde su inicio hasta ese momento. La información sobre todos los eventos que ocurren durante la tarea se registra en el registro de tareas (consulte la sección "Acerca de los registros de tareas" en la página 200).

► *Para ver estadísticas de la tarea Uso de KSN, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**.
2. Seleccione el nodo secundario **Uso de KSN**.

Las estadísticas de la tarea se muestran en la sección **Estadísticas** del panel de detalles del nodo

seleccionado.

Puede consultar la información sobre objetos procesados por Kaspersky Embedded Systems Security desde que la tarea se inició (consulte la tabla a continuación).

Tabla 46. Estadísticas de la tarea Uso de KSN

Campo	Descripción
Errores de envío de solicitudes	Cantidad solicitudes de KSN cuyo procesamiento produjo un error de la tarea.
Estadísticas creadas	Número de paquetes estadísticos generados enviados a KSN.
Objetos eliminados	Número de objetos que Kaspersky Embedded Systems Security eliminó al ejecutar la tarea Uso de KSN.
Objetos pasados a Copia de seguridad	La cantidad de copias de objetos que Kaspersky Embedded Systems Security guardó en Copia de seguridad.
Objetos no eliminados	Cantidad de objetos que Kaspersky Embedded Systems Security intentó eliminar, pero no pudo hacerlo debido a que, por ejemplo, el acceso al objeto estaba bloqueado por otra aplicación. La información sobre tales objetos se registra en el registro de tareas.
Objetos sin copia de seguridad	Una cantidad de objetos cuyas copias Kaspersky Embedded Systems Security intentó guardar en Copia de seguridad, pero no pudo hacerlo; por ejemplo, debido a espacio insuficiente en el disco. La aplicación no desinfecta ni elimina archivos que no se pueden mover a las Copia de seguridad. La información sobre tales objetos se registra en el registro de tareas.
Modo limitado	El estado significa si la aplicación envía solicitudes de reputación de archivos en un modo limitado.

Control de inicio de aplicaciones

Esta sección contiene información acerca de la tarea de Control de inicio de aplicaciones y cómo configurarla.

En este capítulo

Acerca de la tarea Control de inicio de aplicaciones

Al ejecutar la tarea Control de inicio de aplicaciones, Kaspersky Embedded Systems Security supervisa los intentos del usuario de iniciar aplicaciones y permite o deniega el inicio de estas aplicaciones. La tarea Control de inicio de aplicaciones confía en el principio Denegar por defecto, que significa que cualquier aplicación que no esté permitida en la configuración de la tarea se bloqueará automáticamente.

Puede autorizar el inicio de las aplicaciones con uno de los siguientes métodos:

- Definir reglas de autorización para aplicaciones de confianza.
- Comprobar la reputación de aplicaciones de confianza en KSN al iniciarlas.

La tarea le da máxima prioridad a denegar el inicio de las aplicaciones. Por ejemplo, si una aplicación no puede iniciarse por una de las reglas de bloqueo, se denegará el inicio de la aplicación independientemente de la conclusión de confianza para KSN. En ese momento, si los servicios de KSN consideran que la aplicación no es de confianza, pero está incluida en el alcance de la regla de autorización, este inicio de aplicación será denegado.

Todos los intentos de iniciar aplicaciones se registran en el registro de tareas (consulte la sección “Acerca de los registros de tareas”, en la página 200).

La tarea Control de inicio de aplicaciones puede funcionar en uno de los dos modos siguientes:

- **Activar**. Kaspersky Embedded Systems Security usa un conjunto de reglas para controlar el inicio de aplicaciones que entran dentro del alcance de las reglas de la tarea de Control de inicio de aplicaciones. El alcance de las reglas de Control de inicio de aplicaciones se especifica en la configuración de esta tarea. Si una aplicación entra dentro del alcance de la regla de la tarea Control de inicio de aplicaciones y su configuración no satisface ninguna regla especificada, tal inicio de aplicación se denegará.

  Los inicios de las aplicaciones que no entran dentro del alcance de uso de ninguna regla especificada en

la configuración de la tarea de Control de inicio de aplicaciones se autorizan, independientemente de la configuración de la tarea de Control de inicio de aplicaciones.

La tarea **Control de inicio de aplicaciones** no se puede iniciar en el modo Activo si no se ha creado ninguna regla o si hay más de 65,535 reglas para un equipo.

- **Solo estadísticas**. Kaspersky Embedded Systems Security no utiliza reglas de Control de inicio de aplicaciones para permitir o denegar el inicio de aplicaciones. En cambio, solo registra la información sobre inicios de aplicación, las reglas cumplidas por aplicaciones en ejecución y las acciones que se hubieran realizado si la tarea se ejecutara en el modo **Activar**. Se permite el inicio de todas las aplicaciones. Este modo está configurado de forma predeterminada.

  Puede utilizar este modo para crear Reglas de Control de inicio de aplicaciones (consulte la sección “Creación de reglas de permiso para eventos de la tarea Control de inicio de aplicaciones”, en la página 329) según la información del registro de tareas.

Puede configurar la tarea Control de inicio de aplicaciones según uno de los siguientes escenarios:

- La configuración de reglas avanzada (consulte la sección “Acerca de las reglas de Control de inicio de aplicaciones”, en la página 285) y su uso para el control de inicio de aplicaciones.
- La configuración de reglas básica y el uso de KSN (consulte la sección “Configuración del uso de KSN”, en la página 322) para el control de inicio de aplicaciones.

Si los archivos del sistema operativo se encuentran dentro del alcance de la tarea Control de inicio de aplicaciones, le recomendamos que al crear reglas de Control de inicio de aplicaciones se asegure que tales aplicaciones estén permitidas por las reglas recién creadas. De otra forma, es posible que el sistema operativo tenga un error al iniciarse.

Kaspersky Embedded Systems Security también intercepta los procesos iniciados en el subsistema Windows para Linux (excepto en el caso de scripts ejecutados desde el shell de UNIX™ o intérpretes de línea de comandos). Para tales procesos, la tarea Control de inicio de aplicaciones aplica la acción definida por la configuración actual. La tarea Generador de reglas para Control de inicio de aplicaciones detecta los inicios de aplicaciones y genera las reglas correspondientes para las aplicaciones que se ejecutan en el subsistema Windows para Linux.

Acerca de las reglas de Control de inicio de aplicaciones

Cómo funcionan las reglas de Control de inicio de aplicaciones

La operación de las Reglas de Control de inicio de aplicaciones se basa en los componentes siguientes:

- Tipo de regla.

  Las reglas de Control de inicio de aplicaciones pueden permitir o denegar el inicio de una aplicación. En consecuencia, se las llama reglas de *autorización* o *denegación*. Para crear una lista de reglas de autorización para el Control de inicio de aplicaciones, puede usar el Generador de reglas para generar reglas de autorización o la tarea Control de inicio de aplicaciones en el modo **Solo estadísticas**. También puede agregar las reglas de autorización manualmente.

- Usuario o grupo de usuarios.

  Las reglas de Control de inicio de aplicaciones pueden controlar el inicio de aplicaciones especificadas por

un usuario y/o grupo de usuarios.

- Área de aplicación de regla.

  Las reglas de Control de inicio de aplicaciones pueden aplicarse a *archivos ejecutables*, *scripts* y *paquetes MSI*.

- Criterio de activación de la regla.

  Las reglas de Control de inicio de aplicaciones controlan el inicio de archivos que satisfacen uno de los criterios especificados en la configuración de reglas: está firmado por el *certificado digital* especificado, coincide con el *hash SHA256* especificado o está ubicado en la *ruta* especificada.

  Si el **Certificado digital** se configura como el criterio de activación de la regla, la regla creada controla el inicio de todas las aplicaciones de confianza en el sistema operativo. Puede establecer condiciones más estrictas para este criterio si selecciona las siguientes casillas de verificación:

  - **Usar sujeto**

    La casilla de verificación habilita o deshabilita el uso del asunto del certificado digital como el criterio de activación de la regla.

    Si la casilla de verificación está seleccionada, el asunto especificado del certificado digital se utiliza como el criterio de activación de la regla. La regla creada controlará el inicio de aplicaciones solo para el proveedor especificado en el asunto.

    Si la casilla de verificación está desactivada, la aplicación no usará el asunto del certificado digital como el criterio de activación de una regla. Si se selecciona el criterio **Certificado digital**, la regla creada controlará el inicio de aplicaciones firmadas con un certificado digital que contenga cualquier asunto.

    El asunto del certificado digital utilizado para firmar el archivo solo puede especificarse desde las propiedades del archivo seleccionado con el botón **Establecer criterio de activación de la regla a partir de las propiedades de un archivo**, ubicado arriba de la sección **Criterio de activación de la regla**.

    De forma predeterminada, la casilla está desactivada.

  - **Usar huella**

    La casilla de verificación habilita y deshabilita el uso de la huella del certificado digital como el criterio de activación de la regla.

    Si la casilla de verificación está seleccionada, la huella especificada del certificado digital se utiliza como el criterio de activación de la regla. La regla creada controlará el inicio de aplicaciones firmadas con un certificado digital con la huella especificada.

    Si la casilla de verificación está desactivada, la aplicación no usará la huella del certificado digital como el criterio de activación de una regla. Si se selecciona el criterio **Certificado digital**, la aplicación controlará el inicio de aplicaciones firmadas con un certificado digital que contenga cualquier huella.

    La huella del certificado digital utilizada para firmar el archivo solo puede especificarse desde las propiedades del archivo seleccionado con el botón **Establecer criterio de activación de la regla a partir de las propiedades de un archivo**, ubicado arriba de la sección **Criterio de activación de la regla**.

    De forma predeterminada, la casilla está desactivada.

Las huellas permiten reglas de inicio de la aplicación más restrictivas según un certificado digital, porque una huella identifica en forma exclusiva a un certificado digital y no se puede falsificar, a diferencia del asunto de un certificado digital.

Puede especificar exclusiones para las Reglas de Control de inicio de aplicaciones. Las exclusiones a las Reglas de Control de inicio de aplicaciones se basan en los mismos criterios utilizados para activar las reglas: el certificado digital, el hash SHA256 y la ruta de archivo. Pueden requerirse exclusiones a las reglas de Control de inicio de aplicaciones para ciertas reglas de autorización: por ejemplo, si desea autorizar que usuarios inicien aplicaciones desde la ruta C:\Windows y, al mismo tiempo, bloquear el inicio del archivo Regedit.exe.

Si los archivos del sistema operativo se encuentran dentro del alcance de la tarea Control de inicio de aplicaciones, le recomendamos que al crear reglas de Control de inicio de aplicaciones se asegure que tales aplicaciones estén permitidas por las reglas recién creadas. De otra forma, es posible que el sistema operativo tenga un error al iniciarse.

Administración de Reglas de Control de inicio de aplicaciones

Puede realizar las siguientes acciones con las Reglas de Control de inicio de aplicaciones:

- Agregar reglas manualmente
- Generar y agregar reglas automáticamente
- Eliminar reglas
- Exportar reglas a un archivo
- Examinar archivos seleccionados para ver reglas que permiten la ejecución de estos archivos.
- Filtrar reglas en la lista según el criterio especificado

Acerca del control de distribución de software

La generación de las reglas de Control de inicio de aplicaciones puede ser complicada si también tiene que controlar la distribución del software en un equipo protegido, por ejemplo, en equipos donde el software instalado se actualiza periódicamente en forma automática. En este caso, se debe actualizar la lista de reglas de autorización después de cada actualización de software para que los archivos creados recientemente se consideren en la configuración de la tarea Control de inicio de aplicaciones. Para simplificar el control de inicio en situaciones de distribución de software, puede usar el subsistema de Control de distribución de software.

Un *paquete de distribución de software* (en adelante, denominado “paquete”) representa una aplicación de software que se instala en un equipo. Cada paquete contiene al menos una aplicación, y también puede contener archivos individuales, actualizaciones o hasta un comando individuales, además de las aplicaciones, en particular cuando se instala una aplicación o una actualización de software.

El subsistema de Control de distribución de software se implementa como lista de exclusiones adicional. Cuando agrega un paquete de distribución del software a esta lista, la aplicación permite que estos paquetes de confianza se descompriman y permite que el software instalado o modificado por un paquete de confianza se inicie automáticamente. Los archivos extraídos pueden heredar el atributo de confianza de un paquete de distribución principal. Un *paquete de distribución principal* es un paquete que el usuario agregó a la lista de exclusiones de Control de distribución de software y se convirtió en un paquete de confianza.

Kaspersky Embedded Systems Security controla solo los ciclos completos de distribución de software. La aplicación no puede procesar correctamente el inicio de archivos modificados por un paquete de confianza si, cuando el paquete se inicia por primera vez, se desactiva el control de distribución de software o no se instala el componente Control de inicio de aplicaciones.

El Control de distribución de software no está disponible si se desactiva la casilla de verificación **Aplicar reglas a archivos ejecutables** en la configuración de la tarea Control de inicio de aplicaciones.

Caché de distribución del software

Kaspersky Embedded Systems Security utiliza un caché de distribución de software generado dinámicamente ("caché de distribución") para establecer la relación entre paquetes de confianza y archivos creados durante la distribución del software. Cuando un paquete se inicia por primera vez, Kaspersky Embedded Systems Security detecta todos los archivos creados por el paquete durante el proceso de distribución del software y almacena sumas de control del archivo y rutas en el caché de distribución. Entonces se permite a todos los archivos en el caché de distribución iniciarse de forma predeterminada.

No puede revisar, limpiar ni modificar manualmente el caché de distribución mediante la interfaz de usuario. Kaspersky Embedded Systems Security completa y controla el caché.

Puede exportar el caché de distribución a un archivo de configuración (en formato XML) y borrar el caché con opciones de la línea de comandos.

► *Para exportar el caché de distribución a un archivo de configuración, ejecute el siguiente comando:*

```
kavshell appcontrol /config /savetofile:<ruta de acceso completa> /sdc
```

► *Para borrar el caché de distribución, ejecute el siguiente comando:*

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security actualiza el caché de distribución cada 24 horas. Si la suma de control de un archivo anteriormente permitido se cambia, la aplicación elimina el registro de este archivo desde el caché de distribución. Si la tarea Control de inicio de aplicaciones se inicia en un modo Activo, los intentos posteriores de iniciar este archivo se bloquearán. Si se cambia la ruta completa al archivo anteriormente permitido, los intentos subsecuentes de iniciar este archivo no se bloquearán, porque la suma de control se almacena dentro del caché de distribución.

Procesamiento de los archivos extraídos

Todos los archivos extraídos de un paquete de confianza heredan el atributo de confianza sobre el primer inicio del paquete. Si desactiva la casilla después del primer inicio, todos los archivos extraídos del paquete conservarán el atributo heredado. Para reiniciar el atributo heredado para todos los archivos extraídos, debe borrar el caché de distribución y desactivar la casilla de verificación **Permitir el lanzamiento de todos los archivos de esta cadena de extracción de paquetes de distribución** antes de volver a iniciar el paquete de distribución de confianza.

Los archivos y paquetes extraídos creados por un paquete de distribución principal heredan el atributo de confianza, ya que sus sumas de control se agregan al caché de distribución cuando el paquete de distribución del software de la lista de exclusiones se abre por primera vez. Por lo tanto, el propio paquete de distribución y todos

los archivos extraídos de este paquete también serán de confianza. De forma predeterminada, la cantidad de niveles de la herencia del atributo de confianza es ilimitada.

Los archivos extraídos conservarán el atributo de confianza después de reiniciar el sistema operativo.

El procesamiento de archivos se define en la Configuración de Control de distribución de software (consulte la sección “Configuración del Control de distribución de software” en la página 300) mediante la selección o la desactivación de la casilla de verificación **Permitir el lanzamiento de todos los archivos de esta cadena de extracción de paquetes de distribución**.

Por ejemplo, supongamos que agrega un paquete test.msi que contiene varios otros paquetes y aplicaciones a la lista de exclusiones y selecciona la casilla. En este caso, se permite la ejecución y la extracción de todos los paquetes y las aplicaciones contenidos en el paquete test.msi, si contienen otros archivos. Esta situación funciona para archivos extraídos en todos los niveles anidados.

Si agrega un paquete test.msi a la lista de exclusiones y desactiva la casilla de verificación **Permitir el lanzamiento de todos los archivos de esta cadena de extracción de paquetes de distribución**, la aplicación asignará el atributo de confianza solo a los paquetes y archivos ejecutables extraídos directamente de un paquete de confianza principal (en el primer nivel de anidación). Las sumas de control de estos archivos se almacenan en el caché de distribución. Todos los archivos en el segundo nivel de anidación y superiores serán bloqueados por el principio de denegación predeterminada.

Trabajar con la lista de reglas de Control de inicio de aplicaciones

La lista de paquetes de confianza del subsistema de control de distribución de software es una lista de exclusiones que amplifica pero no reemplaza la lista general de reglas de control de inicio de aplicaciones.

Las reglas de denegación de control de inicio de aplicaciones tienen la prioridad más alta: se bloqueará la descompresión del paquete de confianza y el inicio de archivos nuevos o modificados si estos paquetes y archivos están afectados por las reglas de denegación de control del inicio de aplicaciones.

Las exclusiones de control de distribución de software se aplican tanto para paquetes de confianza como para archivos creados o modificados por estos paquetes si no se aplica ninguna regla de denegación en la lista de control de inicio de aplicaciones para esos paquetes y archivos.

Uso de las conclusiones de KSN

Las conclusiones de KSN que un archivo es no confiable tienen una prioridad más alta que las exclusiones de control de distribución de software: la descompresión de paquetes de confianza y el inicio de archivos creados o modificados por estos paquetes se bloquearán si KSN informa que estos archivos son no confiables.

Después de descomprimir los datos de un paquete de confianza, todos los archivos secundarios podrán ejecutarse independientemente del uso de KSN dentro del alcance del control de inicio de aplicaciones. En ese momento, los estados de las casillas de verificaciónDenegar inicio de aplicaciones no confiables según KSN y **Autorizar inicio de aplicaciones confiables según KSN** no afectan el funcionamiento de la casilla de verificación **Permitir el lanzamiento de todos los archivos de esta cadena de extracción de paquetes de distribución**.

Acerca del uso de KSN para la tarea Control de inicio de aplicaciones

Para iniciar la tarea de Uso de KSN, debe aceptar la Declaración de KSN.

Si los datos de KSN sobre la reputación de una aplicación se utilizan por la tarea Control de inicio de aplicaciones, la reputación de la aplicación de KSN se considera un criterio para permitir o denegar el inicio de esa aplicación. Si KSN informa a Kaspersky Embedded Systems Security que una aplicación no es confiable cuando el usuario

intenta iniciar la aplicación, el inicio de la aplicación se denegará. Si KSN informa a Kaspersky Embedded Systems Security que una aplicación es confiable cuando el usuario intenta iniciar la aplicación, el inicio de aplicación se autorizará. KSN puede usarse junto con las reglas de control de inicio de aplicaciones o como un criterio independiente para denegar el inicio de aplicaciones.

Uso de conclusiones de KSN como criterio independiente para denegar el inicio de aplicaciones

Este escenario le permite controlar de manera segura el inicio de aplicaciones en el equipo protegido sin la necesidad de la configuración avanzada de la lista de reglas.

Puede aplicar conclusiones KSN para Kaspersky Embedded Systems Security simultáneamente con la única regla especificada. La aplicación solo permitirá el inicio de aplicaciones que son de confianza en KSN o que están habilitadas por una regla especificada.

Para esta situación, le recomendamos definir una regla de autorización de inicio de aplicaciones basada en un certificado digital.

Se deniega el inicio del resto de las aplicaciones de acuerdo con la directiva Denegar por defecto. La utilización de KSN cuando no hay ninguna regla aplicada protege a un equipo de aplicaciones que KSN considera como amenaza.

Uso de conclusiones de KSN simultáneamente con reglas de control de inicio de aplicaciones

Cuando se usan las conclusiones de KSN simultáneamente con el Control de inicio de aplicaciones, se aplican las siguientes condiciones:

- Kaspersky Embedded Systems Security siempre deniega el inicio de una aplicación si se incluye en alcance de al menos una regla de denegación. Si KSN considera que la aplicación es de confianza, la conclusión correspondiente tiene una prioridad inferior y no se considera; el inicio de la aplicación seguirá denegándose. Esto le permite expandir la lista de aplicaciones no deseadas.
- Kaspersky Embedded Systems Security siempre bloquea el inicio de aplicaciones si este está prohibido para aplicaciones que no sean de confianza en KSN y la aplicación no es de confianza en KSN. Si se define una regla de autorización para la aplicación, tiene una prioridad inferior y no se considera; el inicio de la aplicación seguirá denegándose. Esto protege al equipo de aplicaciones que KSN considera una amenaza, pero no se consideraron durante la configuración inicial de las reglas.

Generación de reglas de control de inicio de aplicaciones

Puede crear listas de reglas de Control de inicio de aplicaciones usando tareas y directivas de Kaspersky Security Center simultáneamente para todos los equipos y los grupos de equipos en la red corporativa. Este guion se recomienda si la red corporativa no tiene una máquina de referencia y no puede crear una lista de reglas de autorización según las aplicaciones instaladas en la máquina de la referencia. También puede ejecutar la tarea Generador de reglas para Control de inicio de aplicaciones localmente a través de la Consola de la aplicación para crear una lista de reglas según las aplicaciones que se ejecutan en un solo equipo.

El componente Control de inicio de aplicaciones se instala con dos reglas de permiso preestablecidas:

- Regla de autorización para scripts y archivos MSI con un certificado de confianza para el sistema operativo.
- Regla de autorización para archivos ejecutables con un certificado de confianza para el sistema operativo.

Puede crear listas de reglas de Control de inicio de aplicaciones del lado de Kaspersky Security Center en uno de dos modos:

- Utilizando la tarea de grupo del Generador de reglas para Control de inicio de aplicaciones.

  En este escenario, una tarea de grupo genera su propia lista de reglas de Control de inicio de aplicaciones para cada equipo en la red y guarda esas listas a un archivo XML en la carpeta compartida especificada. El archivo XML generado por la tarea Generador de reglas para Control de inicio de aplicaciones contiene las reglas de autorización especificadas en la configuración de la tarea antes de que se inicie la tarea. No se creará ninguna regla para las aplicaciones que no estén autorizadas para iniciarse en la configuración de la tarea especificada. El inicio de tales aplicaciones se rechaza de forma predeterminada. Luego, puede importar manualmente la lista creada de reglas en la tarea de Control de inicio de aplicaciones para la directiva de Kaspersky Security Center. Puede configurar una directiva de Kaspersky Security Center para el agregado automático de las reglas creadas a la lista de reglas de Control de inicio de aplicaciones cuando finaliza la tarea de grupo del Generador de reglas para Control de inicio de aplicaciones.

  Puede configurar que las reglas generadas se importen automáticamente en la lista de reglas para la tarea Control de inicio de aplicaciones.

  Este escenario se recomienda cuando tiene que crear listas de reglas de Control de inicio de aplicaciones rápidamente. Le recomendamos configurar el inicio planificado de la tarea de Generador de reglas para Control de inicio de aplicaciones solo si las reglas de autorización aplicadas incluyen carpetas y archivos que usted sabe que están seguros.

  > Antes de usar la tarea de Control de inicio de aplicaciones en la red, asegúrese de que todos los equipos protegidos puedan acceder a una carpeta compartida. Si la directiva de la organización no asegura el uso de una carpeta compartida en la red, le recomendamos iniciar la tarea Generador de reglas para Control de inicio de aplicaciones en un equipo del grupo de equipos de prueba o en una máquina de referencia.

- Según un informe de los eventos de tareas generadas en Kaspersky Security Center por la tarea de Control de inicio de aplicaciones ejecutada en el modo **Solo estadísticas**.

  En este escenario, Kaspersky Embedded Systems Security no deniega el inicio de aplicaciones. En cambio, con el Control de inicio de aplicaciones que se ejecuta en el modo **Solo estadísticas**, informa todos los inicios de aplicaciones autorizados y denegados en todos los equipos de red en la pestaña **Eventos** del servidor de administración del Kaspersky Security Center. Kaspersky Security Center utiliza el registro de tareas para generar una sola lista de eventos en los cuales se haya rechazado el inicio de la aplicación.

  Debe configurar el periodo de ejecución de tareas de modo que todos los escenarios posibles de equipos protegidos y grupos de equipos y, al menos, un reinicio del equipo se realicen durante el periodo especificado. Luego de que se agreguen las reglas a la tarea Control de inicio de aplicaciones, puede importar los datos de inicio de aplicaciones desde el informe de eventos de Kaspersky Security Center guardado (formato TXT) y generar reglas de autorización de Control de inicio de aplicaciones para tales aplicaciones según estos datos.

  Esta acción se recomienda si una red empresarial tiene una gran cantidad de equipos de diferentes tipos (con un software diferente instalado).

- Según los eventos de inicios de aplicaciones denegados que se recibieron a través de Kaspersky Security Center, sin crear ni importar un archivo de configuración.

  Para usar esta función, la tarea Control de Inicio de aplicaciones en el equipo local se debe ejecutar bajo una directiva de Kaspersky Security Center activa. En este caso, todos los eventos en el equipo local se envían al Servidor de administración.

Le recomendamos actualizar la lista de reglas cuando el conjunto de aplicaciones instaladas en equipos de red cambia (por ejemplo, cuando se instalan actualizaciones o se reinstalan sistemas operativos). Le recomendamos

generar una lista actualizada de reglas ejecutando la tarea de Generador de reglas para Control de inicio de aplicaciones o la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas** en equipos del grupo de administración de prueba. El grupo de administración de prueba incluye los equipos requeridos para evaluar el inicio de aplicaciones nuevas antes de que se instalen en equipos de red.

Los archivos XML que contienen listas de reglas de autorización se crean según un análisis de las tareas iniciadas en el equipo protegido. Para agrupar todas las aplicaciones utilizadas en la red al generar listas de reglas, le aconsejamos iniciar la tarea de Generador de reglas para Control de inicio de aplicaciones y la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas** en una máquina de referencia.

Antes de generar las reglas de autorización sobre la base de aplicaciones iniciadas en una máquina de referencia, asegúrese de que la máquina de referencia sea segura y no tenga malware.

Antes de agregar reglas de autorización, seleccione uno de los modos de aplicación de la regla disponibles. La lista de reglas de la directiva de Kaspersky Security Center muestra solo las reglas especificadas por la directiva, sin tener en cuenta el modo de aplicación de la regla. La lista de reglas locales incluye todas las reglas aplicadas, tanto reglas locales como reglas agregadas a través de una directiva.

Configuración predeterminada de la tarea Control de inicio de aplicaciones

De forma predeterminada, la tarea de Control de inicio de aplicaciones tiene la configuración descrita en la tabla a continuación. Puede cambiar los valores de esta configuración.

Tabla 47. Configuración predeterminada de la tarea Control de inicio de aplicaciones

Configuración	Valor predeterminado	Descripción
Modo de la tarea	**Solo estadísticas**. Los registros de la tarea denegar eventos de inicio y autorizaron eventos de inicio según las reglas establecidas. El inicio de aplicaciones no se rechaza.	Puede seleccionar el modo **Activar** después de que se genera la lista final de reglas.
Repita las acciones realizadas durante el inicio del primer archivo en todos los inicios subsiguientes de este archivo.	Aplicado	Puede repetir las acciones realizadas durante el inicio del primer archivo en todos los inicios subsiguientes de este archivo..
Denegar el inicio de los intérpretes de línea de comando si no tienen ningún comando que ejecutar	No aplicado.	Puede denegar el inicio de intérpretes de comandos sin comandos para ejecutar.

Configuración	Valor predeterminado	Descripción
Administración de reglas	**Reemplazar las reglas locales con reglas de las directivas**	Puede seleccionar un modo en el cual las reglas especificadas en una directiva se apliquen junto con las reglas del equipo local.
Área de aplicación de las reglas	La tarea controla el inicio de los archivos ejecutables, los scripts y los paquetes MSI. También controla la carga de módulos DLL.	Puede especificar los tipos de archivos cuyo inicio está controlado por reglas.
Uso de KSN	Los datos de la reputación de la aplicación en KSN no se utilizan.	Puede usar los datos de la reputación de la aplicación en KSN al ejecutar una tarea de Control de inicio de aplicaciones.
Permitir la distribución automática de software para las aplicaciones y los paquetes de la lista	No aplicado.	Puede permitir la distribución de software usando los instaladores y las aplicaciones especificadas en la configuración. De forma predeterminada, la distribución de software solo se permite cuando se usa el servicio de Windows Installer.
Permitir siempre la distribución de software a través de Windows Installer	Aplicado (puede cambiarse solo cuando se habilita la configuración **Permitir la distribución automática de software para las aplicaciones y los paquetes de la lista**).	Puede autorizar cualquier instalación o actualización del software si las operaciones se realizan mediante Windows Installer.
Permitir siempre la distribución de software a través de SCCM mediante Background Intelligent Transfer Service	No aplicado (solo cuando se habilita la configuración **Permitir la distribución automática de software para las aplicaciones y los paquetes de la lista**).	Puede activar o desactivar la distribución automática del software mediante el Administrador de configuración del Centro del sistema.
Inicio de la tarea	La primera ejecución no está programada.	La tarea de Control de inicio de aplicaciones no se inicia automáticamente cuando se inicia de Kaspersky Embedded Systems Security. Puede iniciar la tarea manualmente o configurar un inicio programado.

Tabla 48. Configuración predeterminada de la tarea de Generador de reglas para Control de inicio de aplicaciones

Configuración	Valor predeterminado	Descripción
Prefijo para nombres de reglas de autorización	Idéntico al nombre del equipo en el cual se instala Kaspersky Embedded Systems Security.	Puede cambiar el prefijo por nombres de reglas de autorización.

Configuración	Valor predeterminado	Descripción
Área de aplicación de las reglas de autorización	El área de reglas de autorización incluye las siguientes categorías de archivos de forma predeterminada: • Archivos con la extensión EXE ubicados en las carpetas C:\Windows, C:\Program Files (x86) y C:\Program Files • Paquetes MSI almacenados en la carpeta C:\Windows • Scripts almacenados en la carpeta C:\Windows La tarea también crea reglas para todas las aplicaciones en ejecución, sin tener en cuenta su ubicación ni formato.	Puede cambiar el alcance de la protección al agregar o eliminar rutas de carpeta y al especificar los tipos de archivo que estarán autorizados a iniciarse según las reglas generadas automáticamente. Además, puede ignorar aplicaciones en ejecución al crear reglas de autorización.
Criterios para generación de reglas de autorización	Se utilizan el asunto y la huella del certificado digital; se generan reglas para todos los usuarios y los grupos de usuarios.	Puede usar el Hash SHA256 al generar reglas de autorización. Puede seleccionar un usuario y grupo de usuarios para los cuales las reglas de autorización se deben generar automáticamente.
Acciones después de la finalización de la tarea	Las reglas de autorización se agregan a la lista de reglas de Control de inicio de aplicaciones; las reglas nuevas se fusionan con las reglas existentes y las reglas duplicadas se eliminan.	Puede agregar reglas a las reglas existentes sin fusionarlas y sin eliminar las reglas duplicadas; reemplazar las reglas existentes con reglas de autorización nuevas; o configurar la exportación de reglas de autorización a un archivo.
Configuración del inicio de tareas con permisos	La tarea se inicia con una cuenta de sistema.	Puede autorizar a la tarea de Generador de reglas para Control de inicio de aplicaciones a iniciarse en una cuenta de sistema o utilizando los permisos de un usuario especificado.
Programación de inicio de tareas	La primera ejecución no está programada.	La tarea de Generador de reglas para Control de inicio de aplicaciones no se inicia automáticamente cuando se inicia Kaspersky Embedded Systems Security. Puede iniciar la tarea manualmente o configurar un inicio programado.

Gestión del Control de inicio de aplicaciones a través del Complemento de administración

En esta sección, aprenderá a navegar la interfaz del Complemento de administración y ajustar la configuración de la tarea para uno o todos los equipos en la red.

En esta sección

Navegación

Sepa cómo navegar a la configuración de la tarea requerida a través de la interfaz.

En esta sección

Cómo abrir la configuración de la directiva para la tarea Control de inicio de aplicaciones

► *Para abrir la configuración de la tarea Control de inicio de aplicaciones a través de la directiva de Kaspersky Security Center:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas.**
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Control de actividad local**.
6. Haga clic en el botón **Configurar** en la subsección **Control de inicio de aplicaciones**.

   Se abre la ventana **Control de inicio de aplicaciones**.

Configure la directiva según sea necesario.

Cómo abrir la lista de reglas de Control de inicio de aplicaciones

► *Para abrir la lista de reglas de Control de inicio de aplicaciones a través de Kaspersky Security Center:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.

3. Seleccione la pestaña **Directivas.**
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Control de actividad local**.
6. Haga clic en el botón **Configurar** en la subsección **Control de inicio de aplicaciones**.

   Se abre la ventana **Control de inicio de aplicaciones**.
7. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

   Se abre la ventana **Reglas de Control de inicio de aplicaciones**.

Configure la lista de reglas como sea necesario.

Cómo abrir las propiedades y el asistente de la tarea de Generador de reglas para Control de inicio de aplicaciones

► *Para empezar a crear la tarea de Generador de reglas para Control de inicio de aplicaciones:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Tareas**.
4. Haga clic en el botón **Crear una tarea**.

   Se abre la ventana **Nuevo asistente de tarea**.
5. Seleccione la tarea **Generador de reglas para Control de inicio de aplicaciones**.
6. Haga clic en **Siguiente**.

   Se abre la ventana **Configuración**.

► *Para configurar la tarea Generador de reglas para Control de inicio de aplicaciones:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Tareas**.
4. Haga doble clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

   Se abre la ventana **Propiedades:** Se abre la ventana **Generador de reglas para Control de inicio de aplicaciones**.

Consulte la sección Configuración de la tarea de Generador de reglas para Control de inicio de aplicaciones para obtener más información sobre la configuración de la tarea.

Configuración de la tarea Control de inicio de aplicaciones

► *Para ajustar la configuración general de la tarea Control de inicio de aplicaciones:*

1. Abra la ventana **Control de inicio de aplicaciones** (consulte la sección "**Cómo abrir la configuración de la directiva para la tarea Control de inicio de aplicaciones**" en la página 295).
2. En la pestaña **General**, seleccione la configuración siguiente en la sección **Modo de la tarea**:
   - En la lista desplegable **Modo de la tarea**, especifique el modo de la tarea.

     En esta lista desplegable, puede seleccionar el modo de la tarea de Control de inicio de aplicaciones:

     - **Activar**. Kaspersky Embedded Systems Security utiliza las reglas especificadas para controlar el inicio de cualquier aplicación.
     - **Solo estadísticas**. Kaspersky Embedded Systems Security no utiliza las reglas especificadas para controlar el inicio de las aplicaciones. En cambio, simplemente registra la información sobre eventos de inicio en el registro de tareas. Se permite el inicio de todas las aplicaciones. Puede usar este modo para generar una lista de Reglas de Control de inicio de aplicaciones sobre la base de la información sobre los inicios de aplicaciones denegados en el registro de tareas.

     De forma predeterminada, la tarea Control de inicio de aplicaciones se ejecuta en el modo **Solo estadísticas**.

   - Desactive o seleccione la casilla de verificación **Repetir la acción realizada durante el inicio del primer archivo en todos los inicios subsiguientes de este archivo**.

     La casilla de verificación habilita o deshabilita el control del inicio para los intentos segundos y subsecuentes de iniciar aplicaciones sobre la base de la información sobre eventos almacenada en el caché.

     Si la casilla se selecciona, Kaspersky Embedded Systems Security permite o rechaza los inicios posteriores de una aplicación según la conclusión de la tarea con respecto al primer inicio de la aplicación. Por ejemplo, si las reglas autorizaron el primer inicio de la aplicación, la información sobre esta decisión se almacenará en el caché, y el segundo inicio y todos los inicios subsecuentes también se autorizarán, sin volver a comprobarlo.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza una aplicación cada vez que se intenta el inicio.

     De forma predeterminada, la casilla está activada.

   - Desactive o seleccione la casilla de verificación **Denegar el inicio de los intérpretes de línea de comando si no tienen ningún comando que ejecutar**.

     Si se selecciona la casilla de verificación, Kaspersky Embedded Systems Security deniega el inicio del intérprete de línea de comando aunque el inicio del intérprete esté permitido. Un intérprete de comandos solo se puede iniciar sin comando si se cumplen las dos condiciones siguientes:

     - El inicio del intérprete de línea de comando está autorizado.
     - El comando para ejecutar está autorizado.

     Si se desactiva la casilla de verificación, Kaspersky Embedded Systems Security solo considera las reglas de autorización para el inicio de un intérprete de línea de comando. El inicio se deniega si no se aplica ninguna regla de autorización o el proceso ejecutable no es de confianza para KSN. Si se aplica una regla de autorización o el proceso es de confianza para KSN, se puede iniciar un intérprete de línea de comando con o sin

comando para ejecutar.

Kaspersky Embedded Systems Security reconoce los siguientes intérpretes de línea de comandos:

- cmd.exe
- powershell.exe
- python.exe
- perl.exe

De forma predeterminada, la casilla está desactivada.

3. En la sección **Administración de reglas**, configure las opciones para aplicar reglas:
   a. Haga clic en el botón **Lista de reglas** para agregar reglas de autorización a la tarea de Control de inicio de aplicaciones.

   > Kaspersky Embedded Systems Security no reconoce rutas de acceso que contengan barras invertidas ("/"). Use la barra invertida (“\”) para escribir la ruta de acceso correctamente.

   b. Seleccione el modo para aplicar reglas:

   - **Reemplazar las reglas locales con reglas de las directivas**.

     La aplicación aplica la lista de reglas especificada en la directiva para el control de inicio de aplicaciones centralizado de un grupo de equipos. Las listas de reglas locales no se pueden crear, modificar ni aplicar.

   - **Agregar reglas de la directiva a las reglas locales**.

     La aplicación aplica la lista de reglas especificada en una directiva junto con listas de reglas locales. Puede modificar las listas de reglas locales usando la tarea del Generador de reglas para Control de inicio de aplicaciones.

   > De forma predeterminada, Kaspersky Embedded Systems Security aplica dos reglas predeterminadas que habilitan una lista de scripts, paquetes de MSI y archivos ejecutables si estos objetos están firmados con una firma digital de confianza.

4. En la sección **Área de aplicación de las reglas**, especifique la siguiente configuración:

   - **Aplicar reglas a archivos ejecutables**.

     La casilla activa o desactiva el control de inicio de archivos ejecutables.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security autoriza o bloquea el inicio de archivos ejecutables mediante las reglas especificadas cuya configuración especifica **Archivos ejecutables** como alcance.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no controla el inicio de los archivos ejecutables utilizando las reglas especificadas. Se autoriza el inicio de archivos ejecutables.

     De forma predeterminada, la casilla está activada.

   - **Supervisar la carga de módulos DLL**.

     La casilla activa o desactiva el control de la carga de módulos DLL.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security autoriza o bloquea las cargas de módulos DLL mediante las reglas especificadas cuya

configuración especifica **Archivos ejecutables** como alcance.

Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security no controla la carga de módulos DLL mediante las reglas especificadas. Se autoriza la carga de módulos DLL.

La casilla de verificación se habilita si la casilla de verificación **Aplicar reglas a archivos ejecutables** está seleccionada.

De forma predeterminada, la casilla está desactivada.

El control de la carga de módulos DLL puede afectar el rendimiento del sistema operativo.

- **Aplicar reglas a scripts y paquetes MSI**.

  La casilla de verificación habilita o deshabilita el inicio de scripts y paquetes MSI.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security autoriza o bloquea el inicio de scripts y paquetes MSI mediante las reglas especificadas cuya configuración especifica scripts y paquetes MSI como área.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no controla el inicio de scripts y paquetes MSI mediante las reglas especificadas. Se autoriza el inicio de scripts y paquetes MSI.

  De forma predeterminada, la casilla está activada.

5. En la casilla de grupo **Uso de KSN**, configure las siguientes opciones de inicio de aplicaciones:

   - **Denegar inicio de aplicaciones no confiables según KSN**.

     La casilla de verificación habilita o deshabilita el Control de inicio de aplicaciones según los datos de reputación de la aplicación en KSN.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security bloquea la ejecución de cualquier aplicación si no es de confianza en KSN. Las reglas de autorización de Control de inicio de aplicaciones que se aplican a aplicaciones que no son de confianza en KSN no se iniciarán. Si selecciona la casilla de verificación, se proporciona protección adicional contra el malware.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no toma en cuenta la reputación de aplicaciones que no son de confianza en KSN y autoriza o bloquea el inicio de acuerdo con las reglas que se aplican a tales aplicaciones.

     De forma predeterminada, la casilla está desactivada.

   - **Autorizar inicio de aplicaciones confiables según KSN**.

     La casilla de verificación habilita o deshabilita el Control de inicio de aplicaciones según los datos de reputación de la aplicación en KSN.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security permite que las aplicaciones se ejecuten si son de confianza en KSN. La denegación de reglas de control de inicio de aplicaciones que se aplican a las aplicaciones de confianza de KSN tienen una prioridad más alta: si una aplicación es de confianza para los servicios de KSN, el inicio de la aplicación se rechazará.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no toma en cuenta la reputación de aplicaciones de confianza en KSN y autoriza o deniega el inicio de acuerdo con las reglas que se aplican a tales aplicaciones.

De forma predeterminada, la casilla está desactivada.

- Los usuarios o grupos de usuarios permitieron lanzar aplicaciones de confianza en KSN.

6. En la pestaña **Control de distribución de software**, configure las opciones para control de distribución de software (consulte la sección “Configuración del Control de distribución de software” en la página 300).
7. En la pestaña **Administración de la tarea**, configure las opciones de programación de inicio de tareas (consulte la sección “Configuración de las opciones de programación de inicio de tareas” en la página 128).
8. Haga clic en **Aceptar** en la ventana **Configuración de tareas**.

Kaspersky Embedded Systems Security aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Configuración del Control de distribución de software

► *Para agregar un paquete de distribución de confianza:*

1. Abra la ventana **Control de inicio de aplicaciones** (consulte la sección "Cómo abrir la configuración de la directiva para la tarea Control de inicio de aplicaciones" en la página 295).
2. En la pestaña **Control de distribución de software**, seleccione la casilla de verificación **Permitir la distribución automática de software para las aplicaciones y los paquetes de la lista**.

   La casilla de verificación habilita o deshabilita la creación automática de exclusiones para todos los archivos iniciados y utiliza los paquetes de distribución especificados en la lista.

   Si la casilla está marcada, la aplicación automáticamente permite que se inicien los archivos en los paquetes de distribución de confianza. La lista de aplicaciones y paquetes de distribución autorizadas para ser iniciados se puede editar.

   Si la casilla de verificación está desactivada, la aplicación no aplica las exclusiones especificadas en la lista.

   De forma predeterminada, la casilla está desactivada.

   Puede seleccionar **Permitir la distribución automática de software para las aplicaciones y los paquetes de la lista** si la casilla de verificación **Aplicar reglas a archivos ejecutables** en la pestaña **General** está seleccionada en la configuración de la tarea **Control de inicio de aplicaciones**.

3. Desactive la casilla de verificación **Permitir siempre la distribución de software a través de Windows Installer** si es necesario.

   La casilla de verificación habilita o deshabilita la creación automática de exclusiones para todos los archivos ejecutados mediante Windows Installer.

   Si la casilla está seleccionada, los archivos instalados mediante Windows Installer siempre estarán autorizados a iniciarse.

   Si la casilla está desactivada, los archivos no estarán autorizados a iniciarse incondicionalmente, aunque se inicien mediante Windows Installer.

   De forma predeterminada, la casilla está activada.

   La casilla de verificación no se puede modificar si la casilla **Permitir la distribución automática de software para las aplicaciones y los paquetes de la lista** no está

seleccionada.

Solo se recomienda desactivar la casilla **Permitir siempre la distribución de software a través de Windows Installer** si es absolutamente necesario. Desactivar esta función puede causar errores al actualizar archivos del sistema operativo y también impedir el inicio de archivos extraídos de un paquete de distribución.

4. Si es necesario, seleccione la casilla de verificación **Permitir siempre la distribución de software a través de SCCM mediante Background Intelligent Transfer Service**.

   La casilla activa o desactiva la distribución automática del software mediante el Administrador de configuración del Centro del sistema.

   Si la casilla se selecciona, Kaspersky Embedded Systems Security automáticamente permite la implementación de Microsoft Windows mediante el Administrador de configuración del Centro del sistema. La aplicación permite a distribución del software únicamente mediante el Servicio de Transferencia Inteligente en Segundo Plano.

   Los controles de aplicaciones inician los objetos con las extensiones siguientes:

   - .exe
   - .msi

   De forma predeterminada, la casilla está desactivada.

La aplicación controla el ciclo de distribución del software en el equipo; desde la entrega del paquete hasta la instalación o actualización. La aplicación no controla procesos si alguna etapa de distribución se realizara antes de la instalación de la aplicación en el equipo.

5. Para modificar la lista de paquetes de distribución de confianza, haga clic en **Modificar la lista de paquetes**y seleccione uno de los siguientes métodos en la ventana que se abre:

   - **Agregar un paquete de distribución**.

     a. Haga clic en el botón **Examinar** y seleccione el archivo ejecutable o el paquete de distribución.

        La sección **Criterios de confianza** se completa automáticamente con datos sobre el archivo seleccionado.

     b. Desactive o seleccione la casilla de verificación **Permitir el lanzamiento de todos los archivos de esta cadena de extracción de paquetes de distribución**.

     c. Seleccione una de dos opciones disponibles para criterios para usar para determinar si un archivo o el paquete de distribución es de confianza:

        - **Usar certificado digital**
        - Usar hash SHA256]

   - **Agregar varios paquetes por hash**.

     Puede seleccionar un número ilimitado de archivos de ejecutables y paquetes de distribución, y agregarlos a la lista al mismo tiempo. Kaspersky Embedded Systems Security examina el hash y permite que el sistema operativo inicie los archivos especificados.

   - **Cambiar el paquete seleccionado**.

Use esta opción para seleccionar otro archivo de inicio o paquete de distribución, o bien para cambiar los criterios de confianza.

- **Importar lista de paquetes de distribución desde el archivo**.

  Puede importar la lista de paquetes de distribución de confianza desde un archivo de configuración. Para ser reconocido por Kaspersky Embedded Systems Security, el archivo debe cumplir con los siguientes parámetros:

  - La extensión del archivo debe ser TXT.
  - El archivo contiene información estructurada como una lista de líneas, donde cada línea incluye datos para uno de los archivos de confianza.
  - El archivo debe contener una lista en uno de los formatos siguientes:
    - <nombre de archivo>:<SHA256 hash>.
    - <SHA256 hash>*<nombre de archivo>.

  En la ventana **Abrir**, especifique el archivo de configuración que contiene una lista de paquetes de distribución de confianza.

6. Si desea eliminar una aplicación o un paquete de distribución anteriormente agregados a la lista de confianza, haga clic en el botón **Eliminar paquetes de distribución**. Se podrán ejecutar los archivos extraídos.

   Para impedir que los archivos extraídos se inicien, desinstale la aplicación en el equipo protegido o cree una regla de denegación en la configuración de la tarea Control de inicio de aplicaciones.

7. Haga clic en **Aceptar**.

Se guardan las opciones configuradas recientemente.

Configuración de la tarea de Generador de reglas para Control de inicio de aplicaciones

► *Para configurar la tarea de Generador de reglas para Control de inicio de aplicaciones, siga estos pasos:*

1. Abra la ventana **Propiedades:** Ventana **Generador de reglas para Control de inicio de aplicaciones** (consulte la sección "**Cómo abrir las propiedades y el asistente de la tarea de Generador de reglas para Control de inicio de aplicaciones**" en la página 296).
2. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.

   Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

3. En la sección **Configuración**, puede establecer la siguiente configuración:
   - Agregue un prefijo para nombres de regla.
   - Configure el área de aplicación de las reglas de autorización:
     - Crear reglas de autorización para las aplicaciones en ejecución;
     - Crear reglas de autorización para las aplicaciones de las carpetas específicas.

4. En la sección **Opciones**, puede especificar las acciones que desea realizar mientras crea reglas de autorización de Control de inicio de aplicaciones:

   - **Usar certificado digital**

     Si esta opción está seleccionada, se especifica la presencia de un certificado digital como un criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inician mediante archivos con un certificado digital. Recomendamos esta opción si desea autorizar el inicio de alguna aplicación de confianza en el sistema operativo.

     De forma predeterminada, esta opción está seleccionada.

   - **Usar sujeto y huella digital del certificado digital**

     La casilla de verificación habilita o deshabilita el uso del asunto y la huella del certificado digital del archivo como criterio para activar las reglas de autorización para el Control de inicio de aplicaciones. Seleccionar esta casilla de verificación le permite especificar condiciones más estrictas de verificación del certificado digital.

     Si esta casilla de verificación está seleccionada, los valores del asunto y de la huella del certificado digital de los archivos para los cuales se generan las reglas se configuran como criterio de activación de las reglas de autorización para el Control de inicio de aplicaciones. Kaspersky Embedded Systems Security autorizará las aplicaciones que se inicien mediante archivos con la huella y certificado digital especificados.

     Seleccionar esta casilla de verificación restringe altamente la activación de reglas de autorización sobre la base de un certificado digital, ya que una huella es un identificador exclusivo de un certificado digital y no se puede falsificar.

     Si esta casilla de verificación está desactivada, la existencia de cualquier certificado digital de confianza en el sistema operativo se configura como criterio de activación de las reglas de autorización para el Control de inicio de aplicaciones.

     Esta casilla de verificación está activa si la opción **Usar certificado digital** está seleccionada.

     De forma predeterminada, la casilla está activada.

   - **De no haber un certificado, usar**

     Esta es una lista desplegable que le permite seleccionar el criterio de activación de una regla de autorización para el Control de inicio de aplicaciones si el archivo utilizado para generar la regla no tiene ningún certificado digital.

     - **Hash SHA256**. El valor de la suma de control del archivo utilizado para generar la regla se configura como criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación permitirá el inicio de programas que se inicien mediante archivos con la suma de control especificada.
     - **ruta de acceso al archivo**. La ruta de acceso al archivo utilizado para generar la regla se configura como criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inicien con archivos ubicados en las carpetas especificada en la tabla **Crear reglas de autorización para las aplicaciones de las siguientes carpetas** en la sección **Configuración**.

   - **Usar hash SHA256**

     Si esta opción está seleccionada, la suma de control del archivo utilizada para generar la regla se especifica como un criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de inicio de aplicaciones. La aplicación permitirá el inicio de

programas que se inicien mediante archivos con la suma de control especificada.

Recomendamos esta opción para los casos donde las reglas generadas deben conseguir el mayor nivel de seguridad: una suma de control de SHA256 se puede utilizar como ID de archivo único. El uso de una suma de control de SHA256 como criterio de activación de la regla restringe el área de aplicación de la regla a un archivo.

De forma predeterminada, esta opción está desactivada.

- **Generar reglas para este usuario o grupo de usuarios**.

  Este es un campo que muestra a un usuario o grupo de usuarios. La aplicación controlará las aplicaciones ejecutadas por el usuario especificado o el grupo de usuarios.

  La selección predeterminada es **Todos**.

Puede establecer la configuración para archivos de configuración con listas de reglas de autorización que Kaspersky Embedded Systems Security crea después de la finalización de la tarea.

1. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
2. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para la ejecución de la tarea.
3. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones del área de la tarea**.

   Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

4. En la ventana **Propiedades: <Nombre de la tarea>**, haga clic en **Aceptar**.

   Se guardan las opciones de las tareas de grupo recientemente configuradas.

Configuración de las reglas de Control de inicio de aplicaciones a través de Kaspersky Security Center

Aprenda a generar una lista de reglas según distintos criterios o a crear manualmente reglas de autorización o denegación utilizando la tarea Control de inicio de aplicaciones.

En esta sección

Adición de una regla de Control de inicio de aplicaciones

► *Para agregar una regla de Control de inicio de aplicaciones:*

1. Abra la ventana **Reglas de Control de inicio de aplicaciones** (consulte la sección "Cómo abrir la lista de reglas de Control de inicio de aplicaciones" en la página 295).
2. Haga clic en el botón **Agregar**.
3. En el menú contextual del botón, seleccione **Agregar una regla**.

   Se abre la ventana **Configuración de regla**.
4. Especifique la siguiente configuración:
   a. En el campo **Nombre**, ingrese el nombre de la regla.
   b. En la lista desplegable **Tipo**, seleccione el tipo de regla:
      - **De autorización** si desea que la regla autorice el inicio de aplicaciones de acuerdo con los criterios especificados en la configuración de reglas.
      - **De denegación** si desea que la regla bloquee el inicio de aplicaciones de acuerdo con los criterios especificados en la configuración de reglas.
   c. En la lista desplegable **Área**, seleccione el tipo de archivos cuya ejecución será controlada por la regla:
      - **Archivos ejecutables** si desea que la regla controle el inicio de archivos ejecutables.
      - **Scripts y paquetes MSI** si desea que la regla controle el inicio de scripts y paquetes MSI.
   d. En el campo **Usuario o grupo de usuarios**, especifique los usuarios a quienes se autorizará o se denegará iniciar programas según el tipo de regla. Para ello, realice las siguientes acciones:
      i. Haga clic en el botón **Examinar**.
      ii. Se abre la ventana estándar **Seleccionar usuarios o grupos** de Microsoft Windows.
      iii. Especifique la lista de usuarios o grupos de usuarios.
      iv. Haga clic en **Aceptar**.
   e. Si desea tomar los valores de los criterios de activación de la regla enumerados en la sección **Criterio de activación de la regla** de un archivo específico:
      i. Haga clic en el botón **Establecer criterio de activación de la regla a partir de las propiedades de un archivo**.

         Se abre la ventana estándar **Abrir** de Microsoft Windows.
      ii. Seleccione el archivo.
      iii. Haga clic en el botón **Abrir**.

         Los valores de criterios en el archivo se muestran en los campos en la sección **Criterio de activación de la regla**. El criterio para el cual están disponibles los datos en las propiedades del archivo se selecciona de forma predeterminada.

f. En la ventana **Criterio de activación de la regla**, seleccione una de las opciones siguientes:

- **Certificado digital** si desea que la regla controle el inicio de aplicaciones que se inician con archivos firmados con un certificado digital:
  - Seleccione la casilla de verificación **Usar sujeto** si desea que la regla controle el inicio de archivos firmados con un certificado digital solo con el encabezado especificado.
  - Seleccione la casilla de verificación **Usar huella** si desea que la regla controle solo el inicio de archivos firmados con un certificado digital con la huella especificada.
- **Hash SHA256** si desea que la regla controle el inicio de programas que se inician con archivos cuya suma de control coincide con la especificada.
- **Ruta de acceso al archivo** si desea que la regla controle el inicio de programas que se inician con archivos ubicados en la ruta especificada.

  Kaspersky Embedded Systems Security no reconoce rutas de acceso que contengan barras invertidas ("/"). Use la barra invertida (“\”) para escribir la ruta de acceso correctamente.

g. Si desea agregar exclusiones de la regla, realice lo siguiente:

i. En la sección **Exclusiones de la regla**, haga clic en el botón **Agregar**.

Se abre la ventana **Exclusión de la regla**.

ii. En el campo **Nombre**, ingrese el nombre de la exclusión.

iii. Especifique la configuración para la exclusión de archivos de la aplicación de la regla de Control de inicio de aplicaciones. Puede llenar los campos de la configuración desde las propiedades del archivo si hace clic en el botón **Establecer exclusión a partir de las propiedades de un archivo**.

- **Certificado digital**

  Si esta opción está seleccionada, se especifica la presencia de un certificado digital como un criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inician mediante archivos con un certificado digital. Recomendamos esta opción si desea autorizar el inicio de alguna aplicación de confianza en el sistema operativo.

  De forma predeterminada, esta opción está seleccionada.

- **Usar sujeto**

  La casilla de verificación habilita o deshabilita el uso del asunto del certificado digital como el criterio de activación de la regla.

  Si la casilla de verificación está seleccionada, el asunto especificado del certificado digital se utiliza como el criterio de activación de la regla. La regla creada controlará el inicio de aplicaciones solo para el proveedor especificado en el asunto.

  Si la casilla de verificación está desactivada, la aplicación no usará el asunto del certificado digital como el criterio de activación de una regla. Si se selecciona el criterio **Certificado digital**, la regla creada controlará el inicio de aplicaciones firmadas con un certificado digital que contenga cualquier asunto.

  El asunto del certificado digital utilizado para firmar el archivo solo puede especificarse desde las propiedades del archivo seleccionado con el botón **Establecer criterio de activación de la regla a partir de las propiedades de un archivo**, ubicado arriba de la sección **Criterio de activación de la regla**.

  De forma predeterminada, la casilla está desactivada.

- **Usar huella**

  La casilla de verificación habilita y deshabilita el uso de la huella del certificado digital como el criterio de activación de la regla.

  Si la casilla de verificación está seleccionada, la huella especificada del certificado digital se utiliza como el criterio de activación de la regla. La regla creada controlará el inicio de aplicaciones firmadas con un certificado digital con la huella especificada.

  Si la casilla de verificación está desactivada, la aplicación no usará la huella del certificado digital como el criterio de activación de una regla. Si se selecciona el criterio **Certificado digital**, la aplicación controlará el inicio de aplicaciones firmadas con un certificado digital que contenga cualquier huella.

  La huella del certificado digital utilizada para firmar el archivo solo puede especificarse desde las propiedades del archivo seleccionado con el botón **Establecer criterio de activación de la regla a partir de las propiedades de un archivo**, ubicado arriba de la sección **Criterio de activación de la regla**.

  De forma predeterminada, la casilla está desactivada.

- **Hash SHA256**

  Si esta opción está seleccionada, la suma de control del archivo utilizada para generar la regla se especifica como un criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de inicio de aplicaciones. La aplicación permitirá el inicio de programas que se inicien mediante archivos con la suma de control especificada.

  Recomendamos esta opción para los casos donde las reglas generadas deben conseguir el mayor nivel de seguridad: una suma de control de SHA256 se puede utilizar como ID de archivo único. El uso de una suma de control de SHA256 como criterio de activación de la regla restringe el área de aplicación de la regla a un archivo.

  De forma predeterminada, esta opción está desactivada.

- **Ruta de acceso al archivo**

  Si la casilla se selecciona, Kaspersky Embedded Systems Security usará la ruta de acceso completa al archivo para determinar si el proceso es de confianza.

  Si la casilla de verificación está desactivada, la ruta al archivo no se utiliza para determinar si el proceso es de confianza.

  De forma predeterminada, la casilla está desactivada.

iv. Haga clic en **Aceptar**.

v. Si es necesario, repita los pasos (i) al (iv) para agregar exclusiones adicionales.

5. Haga clic en **Aceptar** en la ventana **Configuración de regla**.

La regla creada se mostrará en la lista de la ventana **Reglas de Control de inicio de aplicaciones**.

Habilitación del modo Habilitación predeterminada

El modo Habilitación predeterminada permite que todas las aplicaciones se inicien si no están bloqueados por reglas o por una conclusión de KSN de que no son confiables. Para activar el modo Habilitación predeterminada, agregue reglas de permiso específicas. Puede activar Habilitación predeterminada solo para scripts o para todos los archivos ejecutables.

► *Para agregar una regla de Habilitación predeterminada:*

1. Abra la ventana **Reglas de Control de inicio de aplicaciones** (consulte la sección "**Cómo abrir la lista de reglas de Control de inicio de aplicaciones**" en la página 295).
2. Haga clic en el botón **Agregar** y, en el menú contextual del botón, seleccione **Agregar una regla**.

   Se abre la ventana **Configuración de regla**.
3. En el campo **Nombre**, ingrese el nombre de la regla.
4. En la lista desplegable **Tipo**, seleccione el tipo de regla **De autorización**.
5. En la lista desplegable **Área**, seleccione el tipo de archivos cuya ejecución será controlada por la regla:
   - **Archivos ejecutables** si desea que la regla controle el inicio de archivos ejecutables.
   - **Scripts y paquetes MSI** si desea que la regla controle el inicio de scripts y paquetes MSI.
6. En la sección **Criterio de activación de la regla**, seleccione la opción **Ruta de acceso al archivo**.
7. Escriba la siguiente máscara: `?:\`
8. Haga clic en **Aceptar** en la ventana **Configuración de regla**.

Kaspersky Embedded Systems Security aplica el modo de Habilitación predeterminada.

Creación de reglas de autorización desde eventos de Kaspersky Security Center

► *Para generar reglas de autorización para aplicaciones desde eventos de Kaspersky Security Center en Control de inicio de aplicaciones:*

1. Abra la ventana **Reglas de Control de inicio de aplicaciones** (consulte la sección "**Cómo abrir la lista de reglas de Control de inicio de aplicaciones**" en la página 295).
2. Haga clic en el botón **Agregar** y, en el menú contextual del botón, seleccione **Crear reglas de autorización para los eventos de Kaspersky Security Center**.
3. Seleccione el principio para agregar las reglas a la lista de reglas de Control de inicio de aplicaciones creadas previamente:
   - **Agregar a reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
   - **Reemplazar reglas existentes** si desea reemplazar las reglas existentes con las reglas importadas.
   - **Combinar con reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

   Se abre la ventana **Generación de reglas de Control de inicio de aplicaciones**.
4. Configure las siguientes opciones de solicitud:
   - **Dirección del Servidor de administración**
   - **Puerto**
   - **Usuario**
   - **Contraseña**

5. Seleccione los tipos de eventos que desea que use la tarea de generación de la regla:
   - **Modo Solo estadísticas: inicio de aplicación denegado**.
   - **Inicio de la aplicación denegado**.
6. Seleccione el periodo en la lista desplegable **Solicitar eventos generados dentro del periodo**.
7. Haga clic en el botón **Generar reglas**.
8. Haga clic en el botón **Guardar**en la ventana **Reglas de Control de inicio de aplicaciones**.

   La lista de reglas en la tarea de Control de inicio de aplicaciones se completará con reglas nuevas generadas según un dato de sistema del equipo con la Consola de administración de Kaspersky Security Center instalada.

   Si la lista de reglas de Control del inicio de aplicaciones ya se especificó en la directiva, Kaspersky Embedded Systems Security agrega las reglas seleccionadas desde los eventos que bloquean las reglas ya especificadas. Las reglas con el mismo hash no se agregan, ya que todas las reglas de la lista deben ser únicas.

Importación de reglas desde el informe de Kaspersky Security Center sobre aplicaciones bloqueadas

Puede importar datos de inicios de la aplicación bloqueada desde el informe generado en Kaspersky Security Center después de la ejecución de la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas** y usar estos datos para generar una lista de reglas de autorización de Control de inicio de aplicaciones en la directiva configurada.

Al generar un informe sobre eventos que ocurren durante la tarea de Control de inicio de aplicaciones, puede hacer un seguimiento de las aplicaciones cuyo inicio se bloquea.

Al importar datos de un informe sobre aplicaciones bloqueadas en la configuración de la directiva, asegúrese de que la lista que está usando solo contenga aplicaciones cuyo inicio desea autorizar.

► *Para especificar reglas de autorización de Control de inicio de aplicaciones para un grupo de equipos según un informe de aplicaciones bloqueadas de Kaspersky Security Center:*

1. Abra la ventana **Control de inicio de aplicaciones** (consulte la sección "Cómo abrir la configuración de la directiva para la tarea Control de inicio de aplicaciones" en la página 295).
2. En la sección **Modo de la tarea**, seleccione el modo **Solo estadísticas**.
3. En las propiedades de la directiva, en la sección **Notificación de eventos**, asegúrese de que:
   - Para **Eventos Críticos**, el período de retención del registro de tareas para los eventos de **Inicio de la aplicación denegado** supere el período planeado para ejecutar la tarea en el modo **Solo estadísticas** (el valor predeterminado es 30 días).
   - Para eventos con un nivel de importancia de **Advertencia**, el período de retención del registro de tareas para eventos de **Modo Solo estadísticas: inicio de aplicación denegado** supere el período planeado para ejecutar la tarea en el modo **Solo estadísticas** (el valor predeterminado es 30 días).

Cuando el periodo de retención de eventos se agota, la información sobre los eventos registrados se elimina y no se refleja en el archivo del informe. Antes de ejecutar la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas**, asegúrese de que el tiempo de ejecución de la tarea no supere el período configurado para los eventos especificados.

4. Cuando la tarea haya finalizado, exporte los eventos registrados a un archivo TXT:
   a. En el espacio de trabajo del nodo **Servidor de administración** en Kaspersky Security Center, seleccione la pestaña **Eventos**.
   b. Haga clic en el nodo **Crear una selección** crear una selección de eventos basada en el criterio *Bloqueado* para ver las aplicaciones cuyo inicio bloqueará la tarea Control de inicio de aplicaciones.
   c. En el panel de detalles de la selección, haga clic en la lista **Exportar eventos a archivo** para guardar el informe sobre inicios de la aplicación bloqueados a un archivo TXT.

Antes de importar y aplicar el informe generado en una directiva, asegúrese de que el informe solo contenga datos sobre las aplicaciones cuyo inicio desea autorizar.

5. Importe datos sobre inicios de aplicación bloqueados en la tarea de Control de inicio de aplicaciones. Para hacerlo, en las propiedades de la directiva en la configuración de la tarea de Control de inicio de aplicaciones, realice lo siguiente:
   a. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

      Se abre la ventana **Reglas de Control de inicio de aplicaciones**.
   b. Haga clic en el botón **Agregar** y, en el menú contextual del botón, seleccione **Importar datos sobre aplicaciones bloqueadas del informe de Kaspersky Security Center**.
   c. Seleccione el principio para agregar reglas desde la lista creada según el informe de Kaspersky Security Center a la lista de reglas de Control de inicio de aplicaciones configuradas anteriormente:
      - **Agregar a reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
      - **Reemplazar reglas existentes** si desea reemplazar las reglas existentes con las reglas importadas.
      - **Combinar con reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.
   d. En la ventana estándar de Microsoft Windows que se abre, seleccione el archivo TXT al cual se exportaron los eventos del informe de inicios de aplicación bloqueados.
   e. Haga clic en **Aceptar** en las ventanas Reglas de Control de inicio de aplicaciones y **Configuración de tareas**.

Las reglas creadas a partir del informe de Kaspersky Security Center sobre aplicaciones bloqueadas se agregan a la lista de reglas de Control de inicio de aplicaciones.

Importación de reglas de Control de inicio de aplicaciones desde un archivo XML

Puede importar informes generados por la tarea de grupo de Generador de reglas para Control de inicio de aplicaciones y aplicarlos como una lista de reglas de autorización en la directiva que está configurando.

Cuando la tarea de grupo de Generador de reglas para Control de inicio de aplicaciones finaliza, la aplicación exporta las reglas de autorización creadas a archivos XML guardados en la carpeta compartida especificada. Cada archivo con una lista de reglas se crea analizando los archivos ejecutados y las aplicaciones iniciadas en cada equipo independiente en la red corporativa. Las listas contienen reglas de autorización para archivos y aplicaciones cuyo tipo coincide con el tipo especificado en la tarea de grupo de Generador de reglas para Control de inicio de aplicaciones.

► *Para especificar las reglas de autorización del Control de inicio de aplicaciones para un grupo de equipos según una lista de reglas de autorización generada automáticamente:*

1. En la pestaña **Tareas** en el panel de control del grupo de equipos que está configurando, cree una tarea de grupo de Generador de reglas para Control de inicio de aplicaciones o seleccione una tarea existente (consulte la sección "Cómo abrir las propiedades y el asistente de la tarea de Generador de reglas para Control de inicio de aplicaciones" en la página 296).
2. En las propiedades de la tarea de grupo de Generador de reglas para Control de inicio de aplicaciones creada o en el asistente de tareas, especifique la siguiente configuración:
   - En la sección **Notificación**, configure las opciones para guardar el informe de ejecución de la tarea.

     Para obtener instrucciones detalladas sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

   - En la sección **Configuración**, especifique los tipos de aplicaciones cuyo inicio será autorizado por las reglas que se crean. Puede modificar el conjunto de las carpetas que contienen aplicaciones autorizadas: excluya carpetas predeterminadas del área de la tarea o agregue carpetas nuevas manualmente.
   - En la sección **Opciones**, especifique las operaciones que deberá realizar la tarea mientras se esté ejecutando y después de que finalice. Especifique el criterio de generación de la regla y el nombre del archivo al cual se exportarán las reglas generadas.
   - En la sección **Programación**, configure las opciones de programación de inicio de tareas.
   - En la sección **Cuenta**, especifique la cuenta de usuario conforme a la cual se ejecutará la tarea.
   - En la sección **Exclusiones del área de la tarea**, especifique los grupos de equipos que deben excluirse del área de la tarea.

     Kaspersky Embedded Systems Security no crea reglas de autorización para las aplicaciones iniciadas en los equipos excluidos.

3. En la pestaña **Tareas** en el panel de control del grupo de equipos configurados, en la lista de tareas de grupo, seleccione la tarea Generador de reglas para Control de inicio de aplicaciones que creó y haga clic en el botón **Iniciar** para iniciar la tarea.

   Cuando la tarea termine, las listas de reglas de autorización generadas automáticamente se guardan en archivos de XML en una carpeta compartida.

Antes de usar la tarea de Control de inicio de aplicaciones en la red, asegúrese de que todos los equipos protegidos puedan acceder a una carpeta compartida. Si la directiva de la organización no asegura el uso de una carpeta compartida en la red, le recomendamos iniciar la tarea Generador de reglas para Control de inicio de aplicaciones en un equipo del grupo de equipos de prueba o en una máquina de referencia.

4. Para agregar las listas de reglas de autorización generadas a la tarea de Control de inicio de aplicaciones:
   a. Abra la ventana **Reglas de Control de inicio de aplicaciones** (consulte la sección "Cómo abrir la lista de reglas de Control de inicio de aplicaciones" en la página 295).
   b. Haga clic en el botón **Agregar** y, en la lista que se abre, seleccione **Importar reglas desde archivo XML**.
   c. Seleccione el principio para agregar las reglas de autorización generadas automáticamente a la lista de reglas de Control de inicio de aplicaciones creadas anteriormente:
      - **Agregar a reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
      - **Reemplazar reglas existentes** si desea reemplazar las reglas existentes con las reglas importadas.
      - **Combinar con reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.
   d. En la ventana estándar de Microsoft Windows que se abre, seleccione archivos de XML creados después de la finalización de la tarea de grupo de Generador de reglas para Control de inicio de aplicaciones.
   e. Haga clic en **Aceptar** en las ventanas **Reglas de Control de inicio de aplicaciones** y **Configuración de tareas**.
5. Si desea aplicar las reglas creadas para controlar el inicio de aplicaciones, en la directiva en las propiedades de la tarea de Control de inicio de aplicaciones, seleccione el modo **Activo** para la tarea.

Las reglas de autorización generadas automáticamente según ejecuciones de la tarea en cada equipo independiente se aplican a todos los equipos de red abarcados por la directiva configurada. En estos equipos, la aplicación solo permitirá el inicio de las aplicaciones para las cuales se crearon reglas de autorización.

Comprobación del inicio de aplicaciones

Antes de aplicar las reglas de Control de inicio de aplicaciones configuradas, puede probar cualquier aplicación para determinar qué reglas de Control de inicio de aplicaciones son provocadas por esa aplicación.

De forma predeterminada, Kaspersky Embedded Systems Security deniega el inicio de las aplicaciones cuyo inicio no está autorizado por una sola regla. Para evitar la denegación del inicio de aplicaciones importantes, debe crear reglas de autorización para ellas.

Si el inicio de una aplicación está controlado por varias reglas de distintos tipos, se da prioridad a las reglas de denegación: el inicio de una aplicación se rechazará si corresponde a tan solo una regla de denegación.

► *Para evaluar las reglas de Control de inicio de aplicaciones:*

1. Abra la ventana **Reglas de Control de inicio de aplicaciones** (consulte la sección "Cómo abrir la lista de reglas de Control de inicio de aplicaciones" en la página 295).
2. En la ventana que se abre, haga clic en el vínculo **Mostrar reglas del archivo**.

   Se abre la ventana de Microsoft Windows estándar.
3. Seleccione el archivo cuyo control de inicio desea evaluar.

La ruta de acceso al archivo especificado se muestra en el campo de búsqueda. La lista contiene todas las reglas que se activarán cuando se inicie el archivo seleccionado.

Creación de la tarea Generador de reglas para Control de inicio de aplicaciones

► *Para crear y configurar la tarea de Generador de reglas para Control de inicio de aplicaciones:*

1. Abra la ventana **Configurar** en el Nuevo asistente de la tarea (consulte la Sección "Cómo abrir las propiedades y el asistente de la tarea de Generador de reglas para Control de inicio de aplicaciones" en la página 296).
2. Configure lo siguiente:
   - Especifique un **Prefijo para reglas**.

     Esta es la primera parte del nombre de una regla. La segunda parte del nombre de la regla se forma con el nombre del objeto que se autoriza a iniciarse.

     El prefijo predeterminado es el nombre del equipo en el cual se instala Kaspersky Embedded Systems Security. Puede cambiar el prefijo por nombres de reglas de autorización.
   - Configure el área de aplicación de las reglas de autorización (consulte la sección "Restricción del alcance del uso de la tarea" en la página 332).
3. Haga clic en **Siguiente**.
4. Especifique las acciones que Kaspersky Embedded Systems Security debe realizar:
   - Al generar reglas de autorización (consulte la sección “Acciones a realizar durante la generación de reglas automáticas”, en la página 333).
   - Al finalizar la tarea (consulte la sección “Acciones a realizar después de la finalización de la generación de reglas automáticas”, en la página 334).
5. En la ventana **Programación**, configure los ajustes del inicio de la tarea programada.
6. Haga clic en **Siguiente**.
7. En la ventana **Seleccionar una cuenta para ejecutar la tarea**, especifique la cuenta que desea utilizar.
8. Haga clic en **Siguiente**.
9. Defina el nombre de la tarea.

10. Haga clic en **Siguiente**.

    El nombre de la tarea no debe tener más de 100 caracteres y no puede contener los siguientes símbolos:
    " * < > & \ : |

    Se abre la ventana **Finalizar creación de la tarea**.

11. Puede ejecutar la tarea opcionalmente después de que el Asistente finalice, seleccionando la casilla **Ejecutar tarea después de que finalice el asistente**.

12. Haga clic en **Finalizar** para terminar de crear la tarea.

► *Para configurar una regla existente en Kaspersky Security Center,*

abra la ventana **Propiedades: Generador de reglas para Control de inicio de aplicaciones** y ajuste la configuración que se detalló anteriormente.

La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

En esta sección

Restricción del alcance de uso de la tarea

► *Para restringir el área de la tarea de Generador de reglas para Control de inicio de aplicaciones:*

1. Abra la ventana **Propiedades: Generador de reglas para Control de inicio de aplicaciones** (consulte la sección "Cómo abrir las propiedades y el asistente de la tarea de Generador de reglas para Control de inicio de aplicaciones" en la página 296).
2. Defina los siguientes valores de configuración de tarea:
   - **Crear reglas de autorización para las aplicaciones en ejecución**.

     Esta casilla habilita o deshabilita la generación de reglas de Control de inicio de aplicaciones para aplicaciones que ya están en ejecución. Esta opción se recomienda si el equipo tiene un conjunto de referencia de aplicaciones sobre la base del cual desea crear reglas de autorización.

     Si esta casilla de verificación está seleccionada, las reglas de autorización para el Control de inicio de aplicaciones se generan a partir de las aplicaciones en ejecución.

     Si esta casilla de verificación está desactivada, las aplicaciones en ejecución no se consideran al generar las reglas de autorización.

De forma predeterminada, la casilla está activada.

Esta casilla de verificación no se puede desactivar si ninguna de las carpetas está seleccionada en la tabla **Crear reglas de autorización para las aplicaciones de las siguientes carpetas**.

- **Crear reglas de autorización para las aplicaciones de las siguientes carpetas**.

  Puede usar la tabla para seleccionar o especificar carpetas para la tarea y los tipos de archivos ejecutables que deben tomarse en cuenta al crear reglas de Control de inicio de aplicaciones. La tarea generará reglas de autorización para archivos de los tipos seleccionados que se ubiquen en las carpetas especificadas.

3. Haga clic en **Aceptar**.

Se guarda la configuración especificada.

Acciones a realizar durante la generación de reglas automáticas

► *Para configurar las acciones que Kaspersky Embedded Systems Security debe realizar durante la ejecución de la tarea de Generador de reglas para Control de inicio de aplicaciones):*

1. Abra la ventana **Propiedades:** Ventana **Generador de reglas para Control de inicio de aplicaciones** (consulte la sección "**Cómo abrir las propiedades y el asistente de la tarea de Generador de reglas para Control de inicio de aplicaciones**" en la página 296).
2. Abra la pestaña **Opciones**.
3. En la sección **Durante la generación de reglas de autorización**, configure las siguientes opciones:

   - **Usar certificado digital**

     Si esta opción está seleccionada, se especifica la presencia de un certificado digital como un criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inician mediante archivos con un certificado digital. Recomendamos esta opción si desea autorizar el inicio de alguna aplicación de confianza en el sistema operativo.

     De forma predeterminada, esta opción está seleccionada.

   - **Usar sujeto y huella digital del certificado digital**

     La casilla de verificación habilita o deshabilita el uso del asunto y la huella del certificado digital del archivo como criterio para activar las reglas de autorización para el Control de inicio de aplicaciones. Seleccionar esta casilla de verificación le permite especificar condiciones más estrictas de verificación del certificado digital.

     Si esta casilla de verificación está seleccionada, los valores del asunto y de la huella del certificado digital de los archivos para los cuales se generan las reglas se configuran como criterio de activación de las reglas de autorización para el Control de inicio de aplicaciones. Kaspersky Embedded Systems Security autorizará las aplicaciones que se inicien mediante archivos con la huella y certificado digital especificados.

     Seleccionar esta casilla de verificación restringe altamente la activación de reglas de autorización sobre la base de un certificado digital, ya que una huella es un identificador exclusivo de un certificado digital y no se puede falsificar.

     Si esta casilla de verificación está desactivada, la existencia de cualquier certificado digital de confianza en el sistema operativo se configura como criterio de activación de

las reglas de autorización para el Control de inicio de aplicaciones.

Esta casilla de verificación está activa si la opción **Usar certificado digital** está seleccionada.

De forma predeterminada, la casilla está activada.

- **De no haber un certificado, usar**

  Esta es una lista desplegable que le permite seleccionar el criterio de activación de una regla de autorización para el Control de inicio de aplicaciones si el archivo utilizado para generar la regla no tiene ningún certificado digital.

  - **Hash SHA256**. El valor de la suma de control del archivo utilizado para generar la regla se configura como criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación permitirá el inicio de programas que se inicien mediante archivos con la suma de control especificada.
  - **ruta de acceso al archivo**. La ruta de acceso al archivo utilizado para generar la regla se configura como criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inicien con archivos ubicados en las carpetas especificada en la tabla **Crear reglas de autorización para las aplicaciones de las siguientes carpetas** en la sección **Configuración**.

- **Usar hash SHA256**

  Si esta opción está seleccionada, la suma de control del archivo utilizada para generar la regla se especifica como un criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de inicio de aplicaciones. La aplicación permitirá el inicio de programas que se inicien mediante archivos con la suma de control especificada.

  Recomendamos esta opción para los casos donde las reglas generadas deben conseguir el mayor nivel de seguridad: una suma de control de SHA256 se puede utilizar como ID de archivo único. El uso de una suma de control de SHA256 como criterio de activación de la regla restringe el área de aplicación de la regla a un archivo.

  De forma predeterminada, esta opción está desactivada.

- **Generar reglas para este usuario o grupo de usuarios**.

  Este es un campo que muestra a un usuario o grupo de usuarios. La aplicación controlará las aplicaciones ejecutadas por el usuario especificado o el grupo de usuarios.

  La selección predeterminada es **Todos**.

4. Haga clic en **Aceptar**.

Se guarda la configuración especificada.

Acciones a realizar después de la finalización de la generación de reglas automáticas

► *Para configurar las acciones que realizará Kaspersky Embedded Systems Security después de que finalice la tarea de Generador de reglas para Control de inicio de aplicaciones:*

1. Abra la ventana **Propiedades: Generador de reglas para Control de inicio de aplicaciones** (consulte la sección "Cómo abrir las propiedades y el asistente de la tarea de Generador de reglas para Control de inicio de aplicaciones" en la página 296).
2. Abra la pestaña **Opciones**.

3. En la sección **Después de completada la tarea**, configure las siguientes opciones:

   - **Agregar reglas de autorización a la lista de reglas de Control de inicio de aplicaciones**.

     La casilla de verificación habilita o deshabilita la adición de reglas de autorización recientemente generadas a la lista de reglas de Control de inicio de aplicaciones. La lista de reglas de **Reglas de Control de inicio de aplicaciones** se muestra cuando hace clic en el vínculo Reglas de Control de inicio de aplicaciones en el panel de detalles del nodo Control de inicio de aplicaciones.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security agrega las reglas generadas por la tarea de Generador de reglas para Control de inicio de aplicaciones a la lista de reglas de Control de inicio de aplicaciones según el principio de selección para agregar reglas.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security no agrega las reglas de autorización recientemente generadas a la lista de reglas de Control de inicio de aplicaciones. Las reglas generadas solo se exportan a un archivo.

     De forma predeterminada, la casilla está activada.

   - **Principio de adición**.

     La lista desplegable se utiliza para especificar el método utilizado para agregar las reglas de autorización recientemente generadas a la lista de reglas de Control de inicio de aplicaciones.

     - **Agregar a reglas existentes**. Las reglas se agregan a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
     - **Reemplazar reglas existentes**. Las reglas reemplazan a las reglas existentes en la lista.
     - **Combinar con reglas existentes**. Las reglas se agregan a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

     De forma predeterminada, está seleccionado el método **Combinar con reglas existentes**.

   - **Exportar reglas de autorización a archivo**.

   - **Agregar detalles del equipo al nombre del archivo**.

     La casilla de verificación habilita o deshabilita la adición de información sobre el equipo protegido al nombre del archivo al que se exportarán las reglas de autorización.

     Si esta casilla de verificación está seleccionada, la aplicación agrega el nombre del equipo protegido y la fecha y hora de creación del archivo al nombre del archivo de exportación.

     Si la casilla de verificación está desactivada, la aplicación no agrega información sobre el equipo protegido al nombre del archivo de exportación.

     De forma predeterminada, la casilla está activada.

4. Haga clic en **Aceptar**.

Se guarda la configuración especificada.

Gestión de Control de inicio de aplicaciones a través de la Consola de la aplicación

En esta sección, aprenda a navegar la interfaz de la Consola de la aplicación y establecer la configuración de la tarea en un equipo local.

En esta sección

Navegación

Sepa cómo navegar a la configuración de la tarea requerida a través de la interfaz.

En esta sección

Cómo abrir la configuración de la tarea Control de inicio de aplicaciones

► *Para abrir la configuración de la tarea general de Control de inicio de aplicaciones a través de la Consola de la aplicación:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Control de inicio de aplicaciones**.
3. En el panel de detalles del nodo secundario de **Control de inicio de aplicaciones**, haga clic en el vínculo **Propiedades**.

   Se abre la ventana **Configuración de tareas**.

Cómo abrir la ventana de las reglas de Control de inicio de aplicaciones

► *Para abrir la lista de reglas de Control de inicio de aplicaciones a través de la Consola de la aplicación:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Control de inicio de aplicaciones**.
3. En el panel de detalles del nodo **Control de inicio de aplicaciones**, haga clic en el vínculo **Reglas de Control de inicio de aplicaciones**.

   Se abre la ventana **Reglas de Control de inicio de aplicaciones**.
4. Configure la lista de reglas como sea necesario.

Cómo abrir la configuración de la tarea Generador de reglas para Control de inicio de aplicaciones

► *Para configurar la tarea Generador de reglas para Control de inicio de aplicaciones:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Generadores automatizados de reglas**.
2. Seleccione el nodo secundario **Generador de reglas para Control de inicio de aplicaciones**.
3. En el panel de detalles del nodo secundario **Generador de reglas para Control de inicio de aplicaciones**, haga clic en el vínculo **Propiedades**.

   Se abre la ventana **Configuración de tareas**.
4. Configure la tarea como sea necesario.

Configuración de la tarea Control de inicio de aplicaciones

► *Para ajustar la configuración general de la tarea Control de inicio de aplicaciones:*

1. Abra la ventana **Configuración de tareas** (consulte la sección "Cómo abrir la configuración de la tarea Control de inicio de aplicaciones" en la página 318).
2. Defina los siguientes valores de configuración de tarea:
   - En la pestaña **General**:
     - El modo de la tarea Control de inicio de aplicaciones (consulte la sección “Selección del modo de la tarea Control de inicio de aplicaciones”, en la página 320).
     - El área de aplicación de las reglas en la tarea (consulte la sección "Configuración del área de la tarea de Control de inicio de aplicaciones" en la página 321).
     - El Uso de KSN (consulte la sección "Configuración del uso de KSN" en la página 322).
   - La configuración de Control de distribución de software (consulte la sección "Control de distribución de software" en la página 323) en la pestaña **Control de distribución de software**.
   - La configuración de la programación de inicio de tareas (consulte la sección "Configuración de las opciones de programación de inicio de tareas" en la página 149) en las pestañas **Programación**y **Avanzado**.
3. Haga clic en **Aceptar** en la ventana **Configuración de tareas**.

   La configuración modificada se guarda.

Kaspersky Embedded Systems Security aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

En esta sección

Selección del modo de la tarea Control de inicio de aplicaciones

► *Para configurar el modo de la tarea de Control de inicio de aplicaciones:*

1. Abra la ventana **Configuración de tareas** (consulte la sección "**Cómo abrir la configuración de la tarea Control de inicio de aplicaciones**" en la página 318).
2. En la pestaña **General**, en la lista desplegable **Modo de la tarea**, especifique el modo de la tarea.

   En esta lista desplegable, puede seleccionar un modo de la tarea de Control de inicio de aplicaciones:

   - **Activar**. Kaspersky Embedded Systems Security usa las reglas especificadas para controlar el inicio de cualquier aplicación.
   - **Solo estadísticas**. Kaspersky Embedded Systems Security no utiliza las reglas especificadas para controlar el inicio de las aplicaciones. En cambio, simplemente registra la información sobre esos inicios en el registro de tareas. Todos los programas están autorizados a iniciarse. Puede usar este modo para generar una lista de Reglas de Control de inicio de aplicaciones a partir de la información documentada en el registro de tareas sobre el bloqueo.

   De forma predeterminada, la tarea Control de inicio de aplicaciones se ejecuta en el modo **Solo estadísticas**.
3. Desactive o seleccione la casilla de verificación **Repetir la acción realizada durante el inicio del primer archivo en todos los inicios subsiguientes de este archivo**.

   La casilla de verificación habilita o deshabilita el control del inicio para los intentos segundos y subsecuentes de iniciar aplicaciones sobre la base de la información sobre eventos almacenada en el caché.

   Si la casilla se selecciona, Kaspersky Embedded Systems Security permite o rechaza los inicios posteriores de una aplicación según la conclusión de la tarea con respecto al primer inicio de la aplicación. Por ejemplo, si las reglas autorizaron el primer inicio de la aplicación, la información sobre esta decisión se almacenará en el caché, y el segundo inicio y todos los inicios subsecuentes también se autorizarán, sin volver a comprobarlo.

   Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza una aplicación cada vez que se intenta el inicio.

   De forma predeterminada, la casilla está activada.

   Kaspersky Embedded Systems Security crea una nueva lista de eventos en caché cada vez que se modifica la configuración de la tarea de Control de inicio de aplicaciones. Esto significa que el Control de inicio de aplicaciones se realiza según la configuración de seguridad actual.
4. Desactive o seleccione la opción **Denegar el inicio de los intérpretes de línea de comando si no tienen ningún comando que ejecutar**.

   Si se selecciona la casilla de verificación, Kaspersky Embedded Systems Security deniega el inicio del intérprete de línea de comando aunque el inicio del intérprete esté permitido. Un intérprete de comandos solo se puede iniciar sin comando si se cumplen las dos condiciones siguientes:

   - El inicio del intérprete de línea de comando está autorizado.
   - El comando para ejecutar está autorizado.

   Si se desactiva la casilla de verificación, Kaspersky Embedded Systems Security solo

considera las reglas de autorización para el inicio de un intérprete de línea de comando. El inicio se deniega si no se aplica ninguna regla de autorización o el proceso ejecutable no es de confianza para KSN. Si se aplica una regla de autorización o el proceso es de confianza para KSN, se puede iniciar un intérprete de línea de comando con o sin comando para ejecutar.

Kaspersky Embedded Systems Security reconoce los siguientes intérpretes de línea de comandos:

- cmd.exe
- powershell.exe
- python.exe
- perl.exe

De forma predeterminada, la casilla está desactivada.

5. Haga clic en **Aceptar**.

Se guarda la configuración especificada.

Todos los intentos de iniciar aplicaciones se registran en el registro de tareas.

Configuración del área de la tarea de Control de inicio de aplicaciones

► *Para definir el área de la tarea de Control de inicio de aplicaciones:*

1. Abra la ventana **Configuración de tareas** (consulte la sección "**Cómo abrir la configuración de la tarea Control de inicio de aplicaciones**" en la página 318).
2. En la pestaña **General**, en la sección **Área de aplicación de las reglas**, especifique la siguiente configuración:
   - **Aplicar reglas a archivos ejecutables**

     La casilla activa o desactiva el control de inicio de archivos ejecutables.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security autoriza o bloquea el inicio de archivos ejecutables mediante las reglas especificadas cuya configuración especifica **Archivos ejecutables** como alcance.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no controla el inicio de los archivos ejecutables utilizando las reglas especificadas. Se autoriza el inicio de archivos ejecutables.

     De forma predeterminada, la casilla está activada.

   - **Supervisar la carga de módulos DLL**

     La casilla activa o desactiva el control de la carga de módulos DLL.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security autoriza o bloquea las cargas de módulos DLL mediante las reglas especificadas cuya configuración especifica **Archivos ejecutables** como alcance.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security no controla la carga de módulos DLL mediante las reglas especificadas. Se autoriza la carga de módulos DLL.

La casilla de verificación se habilita si la casilla de verificación **Aplicar reglas a archivos ejecutables** está seleccionada.

De forma predeterminada, la casilla está desactivada.

El control de la carga de módulos DLL puede afectar el rendimiento del sistema operativo.

- **Aplicar reglas a scripts y paquetes MSI**

  La casilla de verificación habilita o deshabilita el inicio de scripts y paquetes MSI.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security autoriza o bloquea el inicio de scripts y paquetes MSI mediante las reglas especificadas cuya configuración especifica scripts y paquetes MSI como área.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no controla el inicio de scripts y paquetes MSI mediante las reglas especificadas. Se autoriza el inicio de scripts y paquetes MSI.

  De forma predeterminada, la casilla está activada.

3. Haga clic en **Aceptar**.

Se guarda la configuración especificada.

Configuración del uso de KSN

► *Para configurar los servicios de uso de KSN para la tarea de Control de inicio de aplicaciones:*

1. Abra la ventana **Configuración de tareas** (consulte la sección "**Cómo abrir la configuración de la tarea Control de inicio de aplicaciones**" en la página 318).
2. En la pestaña **General**, en la sección **Uso de KSN**, especifique la configuración para los servicios de uso de KSN:
   - Si es necesario, seleccione la casilla de verificación **Denegar inicio de aplicaciones no confiables según KSN**.

     La casilla de verificación habilita o deshabilita el Control de inicio de aplicaciones según los datos de reputación de la aplicación en KSN.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security bloquea la ejecución de cualquier aplicación si no es de confianza en KSN. Las reglas de autorización de Control de inicio de aplicaciones que se aplican a aplicaciones que no son de confianza en KSN no se iniciarán. Si selecciona la casilla de verificación, se proporciona protección adicional contra el malware.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no toma en cuenta la reputación de aplicaciones que no son de confianza en KSN y autoriza o bloquea el inicio de acuerdo con las reglas que se aplican a tales aplicaciones.

     De forma predeterminada, la casilla está desactivada.
   - Si es necesario, seleccione la casilla de verificación **Autorizar inicio de aplicaciones confiables según KSN**.

     La casilla de verificación habilita o deshabilita el Control de inicio de aplicaciones según los datos de reputación de la aplicación en KSN.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security

permite que las aplicaciones se ejecuten si son de confianza en KSN. La denegación de reglas de control de inicio de aplicaciones que se aplican a las aplicaciones de confianza de KSN tienen una prioridad más alta: si una aplicación es de confianza para los servicios de KSN, el inicio de la aplicación se rechazará.

Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no toma en cuenta la reputación de aplicaciones de confianza en KSN y autoriza o deniega el inicio de acuerdo con las reglas que se aplican a tales aplicaciones.

De forma predeterminada, la casilla está desactivada.

- Si se la casilla de verificación **Autorizar inicio de aplicaciones confiables según KSN** está seleccionada, indique los usuarios o los grupos de usuarios que pueden iniciar las aplicaciones de confianza en KSN. Para ello, realice las siguientes acciones:

  a. Haga clic en el botón **Editar**.

     Se abre la ventana estándar **Seleccionar usuarios o grupos** de Microsoft Windows.

  b. Especifique la lista de usuarios o grupos de usuarios.

  c. Haga clic en **Aceptar**.

3. Haga clic en **Aceptar** en la ventana **Configuración de tareas**.

Se guarda la configuración especificada.

Control de distribución de software

► *Para agregar un paquete de distribución de confianza:*

1. Abra la ventana **Configuración de tareas** (consulte la sección "**Cómo abrir la configuración de la tarea Control de inicio de aplicaciones**" en la página 318).
2. En la pestaña **Control de distribución de software**, seleccione la casilla de verificación **Permitir la distribución automática de software para las aplicaciones y los paquetes de la lista**.

   La casilla de verificación habilita o deshabilita la creación automática de exclusiones para todos los archivos iniciados y utiliza los paquetes de distribución especificados en la lista.

   Si la casilla está marcada, la aplicación automáticamente permite que se inicien los archivos en los paquetes de distribución de confianza. La lista de aplicaciones y paquetes de distribución autorizadas para ser iniciados se puede editar.

   Si la casilla de verificación está desactivada, la aplicación no aplica las exclusiones especificadas en la lista.

   De forma predeterminada, la casilla está desactivada.

   Puede seleccionar **Permitir la distribución automática de software para las aplicaciones y los paquetes de la lista** si la casilla de verificación **Aplicar reglas a archivos ejecutables** en la pestaña **General** está seleccionada en la configuración de la tarea **Control de inicio de aplicaciones**.

3. Desactive la casilla de verificación **Permitir siempre la distribución de software a través de Windows Installer** si es necesario.

   La casilla de verificación habilita o deshabilita la creación automática de exclusiones para todos los archivos ejecutados mediante Windows Installer.

   Si la casilla está seleccionada, los archivos instalados mediante Windows Installer

siempre estarán autorizados a iniciarse.

Si la casilla está desactivada, los archivos no estarán autorizados a iniciarse incondicionalmente, aunque se inicien mediante Windows Installer.

De forma predeterminada, la casilla está activada.

La casilla de verificación no se puede modificar si la casilla **Permitir la distribución automática de software para las aplicaciones y los paquetes de la lista** no está seleccionada.

Solo se recomienda desactivar la casilla **Permitir siempre la distribución de software a través de Windows Installer** si es absolutamente necesario. Desactivar esta función puede causar errores al actualizar archivos del sistema operativo y también impedir el inicio de archivos extraídos de un paquete de distribución.

4. Si es necesario, seleccione la casilla de verificación **Permitir siempre la distribución de software a través de SCCM mediante Background Intelligent Transfer Service**.

   La casilla activa o desactiva la distribución automática del software mediante el Administrador de configuración del Centro del sistema.

   Si la casilla se selecciona, Kaspersky Embedded Systems Security automáticamente permite la implementación de Microsoft Windows mediante el Administrador de configuración del Centro del sistema. La aplicación permite a distribución del software únicamente mediante el Servicio de Transferencia Inteligente en Segundo Plano.

   Los controles de aplicaciones inician los objetos con las extensiones siguientes:

   - .exe
   - .msi

   De forma predeterminada, la casilla está desactivada.

La aplicación controla el ciclo de distribución del software en el equipo; desde la entrega del paquete hasta la instalación o actualización. La aplicación no controla procesos si alguna etapa de distribución se realizara antes de la instalación de la aplicación en el equipo.

5. Para modificar la lista de paquetes de distribución de confianza, haga clic en **Modificar la lista de paquetes**y seleccione uno de los siguientes métodos en la ventana que se abre:

   - **Agregar un paquete de distribución**.

     a. Haga clic en el botón **Examinar** y seleccione el archivo ejecutable o el paquete de distribución.

        La sección **Criterios de confianza** se completa automáticamente con datos sobre el archivo seleccionado.

     b. Desactive o seleccione la casilla de verificación **Permitir el lanzamiento de todos los archivos de esta cadena de extracción de paquetes de distribución**.

     c. Seleccione una de dos opciones disponibles para criterios para usar para determinar si un archivo o el paquete de distribución es de confianza:

        - **Usar certificado digital**
        - Usar hash SHA256]

   - **Agregar varios paquetes por hash**.

> Puede seleccionar un número ilimitado de archivos de ejecutables y paquetes de distribución, y agregarlos a la lista al mismo tiempo. Kaspersky Embedded Systems Security examina el hash y permite que el sistema operativo inicie los archivos especificados.

- **Cambiar el paquete seleccionado**.

  Use esta opción para seleccionar otro archivo de inicio o paquete de distribución, o bien para cambiar los criterios de confianza.

- **Importar lista de paquetes de distribución desde el archivo**.

  Puede importar la lista de paquetes de distribución de confianza desde un archivo de configuración. Para ser reconocido por Kaspersky Embedded Systems Security, el archivo debe cumplir con los siguientes parámetros:

  - La extensión del archivo debe ser TXT.
  - El archivo contiene información estructurada como una lista de líneas, donde cada línea incluye datos para uno de los archivos de confianza.
  - El archivo debe contener una lista en uno de los formatos siguientes:
    - <nombre de archivo>:<SHA256 hash>.
    - <SHA256 hash>*<nombre de archivo>.

  En la ventana **Abrir**, especifique el archivo de configuración que contiene una lista de paquetes de distribución de confianza.

6. Si desea eliminar una aplicación o un paquete de distribución anteriormente agregados a la lista de confianza, haga clic en el botón **Eliminar paquetes de distribución**. Se podrán ejecutar los archivos extraídos.

   > Para impedir que los archivos extraídos se inicien, desinstale la aplicación en el equipo protegido o cree una regla de denegación en la configuración de la tarea Control de inicio de aplicaciones.

7. Haga clic en **Aceptar**.

Se guardan las opciones configuradas recientemente.

Configuración de las reglas de Control de inicio de aplicaciones

Aprenda cómo generar, importar y exportar una lista de reglas o crear manualmente reglas de autorización o denegación utilizando la tarea de Control de inicio de aplicaciones.

En esta sección

Adición de una regla de Control de inicio de aplicaciones

► *Para agregar una regla de Control de inicio de aplicaciones, siga estos pasos:*

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.
2. Haga clic en el botón **Agregar**.
3. En el menú contextual del botón, seleccione **Agregar una regla**.

   Se abre la ventana **Configuración de regla**.
4. Especifique la siguiente configuración:
   a. En el campo **Nombre**, ingrese el nombre de la regla.
   b. En la lista desplegable **Tipo**, seleccione el tipo de regla:
      - **De autorización** si desea que la regla autorice el inicio de aplicaciones de acuerdo con los criterios especificados en la configuración de reglas.
      - **De denegación** si desea que la regla bloquee el inicio de aplicaciones de acuerdo con los criterios especificados en la configuración de reglas.
   c. En la lista desplegable **Área**, seleccione el tipo de archivos cuya ejecución será controlada por la regla:
      - **Archivos ejecutables** si desea que la regla controle el inicio de archivos ejecutables.
      - **Scripts y paquetes MSI** si desea que la regla controle el inicio de scripts y paquetes MSI.
   d. En el campo **Usuario o grupo de usuarios**, especifique los usuarios a quienes se autorizará o se denegará iniciar programas según el tipo de regla. Para ello, realice las siguientes acciones:
      i. Haga clic en el botón **Examinar**.
      ii. Se abre la ventana estándar **Seleccionar usuarios o grupos** de Microsoft Windows.
      iii. Especifique la lista de usuarios o grupos de usuarios.
      iv. Haga clic en **Aceptar**.
   e. Si desea tomar los valores de los criterios de activación de la regla enumerados en la sección **Criterio de activación de la regla** de un archivo específico:
      i. Haga clic en el botón **Establecer criterio de activación de la regla a partir de las propiedades de un archivo**.

Se abre la ventana estándar **Abrir** de Microsoft Windows.

ii. Seleccione el archivo.

iii. Haga clic en el botón **Abrir**.

Los valores de criterios en el archivo se muestran en los campos en la sección **Criterio de activación de la regla**. El criterio para el cual están disponibles los datos en las propiedades del archivo se selecciona de forma predeterminada.

f. En la ventana **Criterio de activación de la regla**, seleccione una de las opciones siguientes:

- **Certificado digital** si desea que la regla controle el inicio de aplicaciones que se inician con archivos firmados con un certificado digital:
  - Seleccione la casilla de verificación **Usar sujeto** si desea que la regla controle el inicio de archivos firmados con un certificado digital solo con el encabezado especificado.
  - Seleccione la casilla de verificación **Usar huella** si desea que la regla controle solo el inicio de archivos firmados con un certificado digital con la huella especificada.
- **Hash SHA256** si desea que la regla controle el inicio de programas que se inician con archivos cuya suma de control coincide con la especificada.
- **Ruta de acceso al archivo** si desea que la regla controle el inicio de programas que se inician con archivos ubicados en la ruta especificada.

Kaspersky Embedded Systems Security no reconoce rutas de acceso que contengan barras invertidas ("/"). Use la barra invertida (“\”) para escribir la ruta de acceso correctamente.

g. Si desea agregar exclusiones de la regla, realice lo siguiente:

i. En la sección **Exclusiones de la regla**, haga clic en el botón **Agregar**.

Se abre la ventana **Exclusión de la regla**.

ii. En el campo **Nombre**, ingrese el nombre de la exclusión.

iii. Especifique la configuración para la exclusión de archivos de la aplicación de la regla de Control de inicio de aplicaciones. Puede llenar los campos de la configuración desde las propiedades del archivo si hace clic en el botón **Establecer exclusión a partir de las propiedades de un archivo**.

- **Certificado digital**

  Si esta opción está seleccionada, se especifica la presencia de un certificado digital como un criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inician mediante archivos con un certificado digital. Recomendamos esta opción si desea autorizar el inicio de alguna aplicación de confianza en el sistema operativo.

  De forma predeterminada, esta opción está seleccionada.

- **Usar sujeto**

  La casilla de verificación habilita o deshabilita el uso del asunto del certificado digital como el criterio de activación de la regla.

  Si la casilla de verificación está seleccionada, el asunto especificado del certificado digital se utiliza como el criterio de activación de la regla. La regla creada controlará el inicio de aplicaciones solo para el proveedor especificado en el asunto.

Si la casilla de verificación está desactivada, la aplicación no usará el asunto del certificado digital como el criterio de activación de una regla. Si se selecciona el criterio **Certificado digital**, la regla creada controlará el inicio de aplicaciones firmadas con un certificado digital que contenga cualquier asunto.

El asunto del certificado digital utilizado para firmar el archivo solo puede especificarse desde las propiedades del archivo seleccionado con el botón **Establecer criterio de activación de la regla a partir de las propiedades de un archivo**, ubicado arriba de la sección **Criterio de activación de la regla**.

De forma predeterminada, la casilla está desactivada.

- **Usar huella**

  La casilla de verificación habilita y deshabilita el uso de la huella del certificado digital como el criterio de activación de la regla.

  Si la casilla de verificación está seleccionada, la huella especificada del certificado digital se utiliza como el criterio de activación de la regla. La regla creada controlará el inicio de aplicaciones firmadas con un certificado digital con la huella especificada.

  Si la casilla de verificación está desactivada, la aplicación no usará la huella del certificado digital como el criterio de activación de una regla. Si se selecciona el criterio **Certificado digital**, la aplicación controlará el inicio de aplicaciones firmadas con un certificado digital que contenga cualquier huella.

  La huella del certificado digital utilizada para firmar el archivo solo puede especificarse desde las propiedades del archivo seleccionado con el botón **Establecer criterio de activación de la regla a partir de las propiedades de un archivo**, ubicado arriba de la sección **Criterio de activación de la regla**.

  De forma predeterminada, la casilla está desactivada.

- **Hash SHA256**

  Si esta opción está seleccionada, la suma de control del archivo utilizada para generar la regla se especifica como un criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de inicio de aplicaciones. La aplicación permitirá el inicio de programas que se inicien mediante archivos con la suma de control especificada.

  Recomendamos esta opción para los casos donde las reglas generadas deben conseguir el mayor nivel de seguridad: una suma de control de SHA256 se puede utilizar como ID de archivo único. El uso de una suma de control de SHA256 como criterio de activación de la regla restringe el área de aplicación de la regla a un archivo.

  De forma predeterminada, esta opción está desactivada.

- **Ruta de acceso al archivo**

  Si la casilla se selecciona, Kaspersky Embedded Systems Security usará la ruta de acceso completa al archivo para determinar si el proceso es de confianza.

  Si la casilla de verificación está desactivada, la ruta al archivo no se utiliza para determinar si el proceso es de confianza.

  De forma predeterminada, la casilla está desactivada.

iv. Haga clic en **Aceptar**.

v. Si es necesario, repita los pasos (i) al (iv) para agregar exclusiones adicionales.

5. Haga clic en **Aceptar** en la ventana **Configuración de regla**.

La regla creada se mostrará en la lista de la ventana **Reglas de Control de inicio de aplicaciones**.

Habilitación del modo Habilitación predeterminada

El modo Habilitación predeterminada permite que todas las aplicaciones se inicien si no están bloqueados por reglas o por una conclusión de KSN de que no son confiables. Para activar el modo Habilitación predeterminada, agregue reglas de permiso específicas. Puede activar Habilitación predeterminada solo para scripts o para todos los archivos ejecutables.

► *Para agregar una regla de Habilitación predeterminada:*

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.
2. Haga clic en el botón **Agregar**.
3. En el menú contextual del botón, seleccione **Agregar una regla**.

   Se abre la ventana **Configuración de regla**.
4. En el campo **Nombre**, ingrese el nombre de la regla.
5. En la lista desplegable **Tipo**, seleccione el tipo de regla **De autorización**.
6. En la lista desplegable **Área**, seleccione el tipo de archivos cuya ejecución será controlada por la regla:
   - **Archivos ejecutables** si desea que la regla controle el inicio de archivos ejecutables.
   - **Scripts y paquetes MSI** si desea que la regla controle el inicio de scripts y paquetes MSI.
7. En la sección **Criterio de activación de la regla**, seleccione la opción **Ruta de acceso al archivo**.
8. Escriba la siguiente máscara: `?:\`
9. Haga clic en **Aceptar** en la ventana **Configuración de regla**.

Kaspersky Embedded Systems Security aplica el modo de Habilitación predeterminada.

Creación de reglas de autorización desde eventos de la tarea de Control de inicio de aplicaciones

► *Para crear un archivo de configuración que contenga reglas de autorización generadas desde eventos de la tarea de Control de inicio de aplicaciones:*

1. Inicie la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas** (consulte la sección “Selección del modo de la tarea Control de inicio de aplicaciones” en la página 320) para registrar en el registro de tareas la información sobre todos los inicios de aplicaciones en un equipo protegido.
2. Después de que la tarea en el modo **Solo estadísticas** se termina de ejecutar, abra el registro de tareas con un clic en el botón **Abrir el registro de tareas** en la sección **Administración** del panel de detalles del nodo **Control de inicio de aplicaciones**.
3. En la ventana **Registros**, haga clic en **Generar reglas basadas en los eventos**.

Kaspersky Embedded Systems Security generará un archivo XML de configuración que contendrá la lista de reglas según los eventos de la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas**. Puede aplicar esta lista de reglas (consulte la sección “Importación de reglas de Control de aplicaciones desde un archivo XML”, en la página 330) en la tarea Control de inicio de aplicaciones.

Antes de aplicar la lista de reglas generada desde los eventos de la tarea registrados, le recomendamos que revise y procese manualmente la lista para estar seguro que el inicio de archivos críticos (por ejemplo, archivos de sistema) esté autorizado por las reglas especificadas.

Todos los eventos de la tarea se registran en el registro de tareas sin tener en cuenta el modo de la tarea. Puede generar un archivo de configuración con una lista de reglas basado en el registro creado para la tarea que se ejecuta en el modo **Activar**. Este escenario no se recomienda excepto en casos urgentes, porque se debe generar una lista de la regla final antes de que la tarea se ejecute en el modo **Activar** para que sea eficaz.

Exportación de reglas de Control de inicio de aplicaciones

► *Para exportar reglas de Control de inicio de aplicaciones a un archivo de configuración:*

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.
2. Haga clic el botón **Exportar a archivo**.

   Se abre la ventana de Microsoft Windows estándar.
3. En la ventana que se abre, especifique el archivo al cual desea exportar las reglas. Si no existe tal archivo, este se creará. Si ya existe un archivo con el nombre especificado, su contenido se sobrescribirá cuando se exporten las reglas.
4. Haga clic en el botón **Guardar**.

La configuración de la regla se exportará al archivo especificado.

Importación de reglas de Control de inicio de aplicaciones desde un archivo XML

► *Para importar las reglas de Control de inicio de aplicaciones:*

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.
2. Haga clic en el botón **Agregar**.
3. En el menú contextual del botón, seleccione **Importar reglas desde archivo XML**.
4. Especifique el método para agregar reglas importadas. Para hacerlo, seleccione una de las opciones del menú contextual del botón **Importar reglas desde archivo XML**:
   - **Agregar a reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
   - **Reemplazar reglas existentes** si desea reemplazar las reglas existentes con las reglas importadas.
   - **Combinar con reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

   Se abre la ventana estándar **Abrir** de Microsoft Windows.

5. En la ventana **Abrir**, seleccione el archivo XML que contiene las reglas de Control de inicio de aplicaciones.
6. Haga clic en el botón **Abrir**.

Las reglas importadas se mostrarán en la lista en la ventana **Reglas de Control de inicio de aplicaciones**.

Eliminación de reglas de Control de inicio de aplicaciones

► *Para eliminar las Reglas de Control de inicio de aplicaciones:*

1. Abra la ventana de las **Reglas de Control de inicio de aplicaciones**.
2. En la lista, seleccione una o más reglas que desee eliminar.
3. Haga clic en el botón **Eliminar seleccionadas**.
4. Haga clic en el botón **Guardar**.

Las Reglas de Control de inicio de aplicaciones seleccionadas se eliminan.

Configuración de la tarea de Generador de reglas para Control de inicio de aplicaciones

► *Para configurar los ajustes de la tarea de Generador de reglas para Control de inicio de aplicaciones:*

1. Abra la ventana **Configuración de tareas** (consulte la sección "**Cómo abrir la configuración de la tarea Generador de reglas para Control de inicio de aplicaciones**" en la página 319) en la tarea **Generador de reglas para Control de inicio de aplicaciones**.
2. Configure las siguientes opciones:
   - En la pestaña **General**:
     - Especifique un **Prefijo para reglas**.

       Esta es la primera parte del nombre de una regla. La segunda parte del nombre de la regla se forma con el nombre del objeto que se autoriza a iniciarse.

       El prefijo predeterminado es el nombre del equipo en el cual se instala Kaspersky Embedded Systems Security. Puede cambiar el prefijo por nombres de reglas de autorización.
     - Configure el área de aplicación de las reglas de autorización (consulte la sección "Restricción del alcance del uso de la tarea" en la página 332).

- En la pestaña **Acción**, especifique las acciones que Kaspersky Embedded Systems Security debe realizar:
  - Al generar reglas de autorización (consulte la sección “Acciones a realizar durante la generación de reglas automáticas”, en la página 333).
  - Al finalizar la tarea (consulte la sección “Acciones a realizar después de la finalización de la generación de reglas automáticas”, en la página 334).
- En las pestañas **Programación** y **Avanzado**, configure Programar las opciones de inicio de tareas (consulte la sección “Configuración de las opciones de programación de inicio de tareas”, en la página 149).
- En la pestaña **Ejecutar como**, configure las Opciones de inicio de tareas con permisos de la cuenta (consulte la sección “Especificación de una cuenta de usuario para iniciar una tarea” en la página 151).

3. Haga clic en **Aceptar**.

Kaspersky Embedded Systems Security aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación.

En esta sección

Restricción del alcance de uso de la tarea

► *Para restringir el área de la tarea de Generador de reglas para Control de inicio de aplicaciones:*

1. Abra la ventana **Configuración de tareas** (consulte la sección "**Cómo abrir la configuración de la tarea Generador de reglas para Control de inicio de aplicaciones**" en la página 319) en la tarea **Generador de reglas para Control de inicio de aplicaciones**.
2. Defina los siguientes valores de configuración de tarea:
   - **Crear reglas de autorización para las aplicaciones en ejecución**.

     Esta casilla habilita o deshabilita la generación de reglas de Control de inicio de aplicaciones para aplicaciones que ya están en ejecución. Esta opción se recomienda si el equipo tiene un conjunto de referencia de aplicaciones sobre la base del cual desea crear reglas de autorización.

     Si esta casilla de verificación está seleccionada, las reglas de autorización para el Control de inicio de aplicaciones se generan a partir de las aplicaciones en ejecución.

     Si esta casilla de verificación está desactivada, las aplicaciones en ejecución no se consideran al generar las reglas de autorización.

     De forma predeterminada, la casilla está activada.

     Esta casilla de verificación no se puede desactivar si ninguna de las carpetas está seleccionada en la tabla **Crear reglas de autorización para las aplicaciones de las siguientes carpetas**.

- **Crear reglas de autorización para las aplicaciones de las siguientes carpetas**.

  Puede usar la tabla para seleccionar o especificar carpetas para la tarea y los tipos de archivos ejecutables que deben tomarse en cuenta al crear reglas de Control de inicio de aplicaciones. La tarea generará reglas de autorización para archivos de los tipos seleccionados que se ubiquen en las carpetas especificadas.

3. Haga clic en **Aceptar**.

Se guarda la configuración especificada.

Acciones a realizar durante la generación de reglas automáticas

► *Para configurar las acciones que Kaspersky Embedded Systems Security debe realizar durante la ejecución de la tarea de Generador de reglas para Control de inicio de aplicaciones):*

1. Abra la ventana **Configuración de tareas** (consulte la sección "**Cómo abrir la configuración de la tarea Generador de reglas para Control de inicio de aplicaciones**" en la página 319) en la tarea **Generador de reglas para Control de inicio de aplicaciones**.
2. Abra la pestaña **Opciones**.
3. En la sección **Durante la generación de reglas de autorización**, configure las siguientes opciones:

   - **Usar certificado digital**

     Si esta opción está seleccionada, se especifica la presencia de un certificado digital como un criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inician mediante archivos con un certificado digital. Recomendamos esta opción si desea autorizar el inicio de alguna aplicación de confianza en el sistema operativo.

     De forma predeterminada, esta opción está seleccionada.

   - **Usar sujeto y huella digital del certificado digital**

     La casilla de verificación habilita o deshabilita el uso del asunto y la huella del certificado digital del archivo como criterio para activar las reglas de autorización para el Control de inicio de aplicaciones. Seleccionar esta casilla de verificación le permite especificar condiciones más estrictas de verificación del certificado digital.

     Si esta casilla de verificación está seleccionada, los valores del asunto y de la huella del certificado digital de los archivos para los cuales se generan las reglas se configuran como criterio de activación de las reglas de autorización para el Control de inicio de aplicaciones. Kaspersky Embedded Systems Security autorizará las aplicaciones que se inicien mediante archivos con la huella y certificado digital especificados.

     Seleccionar esta casilla de verificación restringe altamente la activación de reglas de autorización sobre la base de un certificado digital, ya que una huella es un identificador exclusivo de un certificado digital y no se puede falsificar.

     Si esta casilla de verificación está desactivada, la existencia de cualquier certificado digital de confianza en el sistema operativo se configura como criterio de activación de las reglas de autorización para el Control de inicio de aplicaciones.

     Esta casilla de verificación está activa si la opción **Usar certificado digital** está seleccionada.

     De forma predeterminada, la casilla está activada.

- **De no haber un certificado, usar**

  Esta es una lista desplegable que le permite seleccionar el criterio de activación de una regla de autorización para el Control de inicio de aplicaciones si el archivo utilizado para generar la regla no tiene ningún certificado digital.

  - **Hash SHA256**. El valor de la suma de control del archivo utilizado para generar la regla se configura como criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación permitirá el inicio de programas que se inicien mediante archivos con la suma de control especificada.
  - **ruta de acceso al archivo**. La ruta de acceso al archivo utilizado para generar la regla se configura como criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inicien con archivos ubicados en las carpetas especificada en la tabla **Crear reglas de autorización para las aplicaciones de las siguientes carpetas** en la sección **Configuración**.

- **Usar hash SHA256**

  Si esta opción está seleccionada, la suma de control del archivo utilizada para generar la regla se especifica como un criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de inicio de aplicaciones. La aplicación permitirá el inicio de programas que se inicien mediante archivos con la suma de control especificada.

  Recomendamos esta opción para los casos donde las reglas generadas deben conseguir el mayor nivel de seguridad: una suma de control de SHA256 se puede utilizar como ID de archivo único. El uso de una suma de control de SHA256 como criterio de activación de la regla restringe el área de aplicación de la regla a un archivo.

  De forma predeterminada, esta opción está desactivada.

- **Generar reglas para este usuario o grupo de usuarios**.

  Este es un campo que muestra a un usuario o grupo de usuarios. La aplicación controlará las aplicaciones ejecutadas por el usuario especificado o el grupo de usuarios.

  La selección predeterminada es **Todos**.

4. Haga clic en **Aceptar**.

Se guarda la configuración especificada.

Acciones a realizar después de la finalización de la generación de reglas automáticas

► *Para configurar las acciones que realizará Kaspersky Embedded Systems Security después de que finalice la tarea de Generador de reglas para Control de inicio de aplicaciones:*

1. Abra la ventana **Configuración de tareas** (consulte la sección "**Cómo abrir la configuración de la tarea Generador de reglas para Control de inicio de aplicaciones**" en la página 319) en la tarea **Generador de reglas para Control de inicio de aplicaciones**.
2. Abra la pestaña **Opciones**.
3. En la sección **Después de completada la tarea**, configure las siguientes opciones:
   - **Agregar reglas de autorización a la lista de reglas de Control de inicio de aplicaciones**.

     La casilla de verificación habilita o deshabilita la adición de reglas de autorización recientemente generadas a la lista de reglas de Control de inicio de aplicaciones. La lista de reglas de **Reglas de Control de inicio de aplicaciones** se muestra cuando hace clic

en el vínculo Reglas de Control de inicio de aplicaciones en el panel de detalles del nodo Control de inicio de aplicaciones.

Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security agrega las reglas generadas por la tarea de Generador de reglas para Control de inicio de aplicaciones a la lista de reglas de Control de inicio de aplicaciones según el principio de selección para agregar reglas.

Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security no agrega las reglas de autorización recientemente generadas a la lista de reglas de Control de inicio de aplicaciones. Las reglas generadas solo se exportan a un archivo.

De forma predeterminada, la casilla está activada.

- **Principio de adición**.

  La lista desplegable se utiliza para especificar el método utilizado para agregar las reglas de autorización recientemente generadas a la lista de reglas de Control de inicio de aplicaciones.

  - **Agregar a reglas existentes**. Las reglas se agregan a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
  - **Reemplazar reglas existentes**. Las reglas reemplazan a las reglas existentes en la lista.
  - **Combinar con reglas existentes**. Las reglas se agregan a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

  De forma predeterminada, está seleccionado el método **Combinar con reglas existentes**.

- **Exportar reglas de autorización a archivo**.

- **Agregar detalles del equipo al nombre del archivo**.

  La casilla de verificación habilita o deshabilita la adición de información sobre el equipo protegido al nombre del archivo al que se exportarán las reglas de autorización.

  Si esta casilla de verificación está seleccionada, la aplicación agrega el nombre del equipo protegido y la fecha y hora de creación del archivo al nombre del archivo de exportación.

  Si la casilla de verificación está desactivada, la aplicación no agrega información sobre el equipo protegido al nombre del archivo de exportación.

  De forma predeterminada, la casilla está activada.

4. Haga clic en **Aceptar**.

Se guarda la configuración especificada.

Control de dispositivos

Esta sección contiene la información sobre la tarea de Control de dispositivos, así como instrucciones para establecer la configuración de la tarea.

En este capítulo

Acerca de la tarea Control de dispositivos

Kaspersky Embedded Systems Security controla el registro y el uso de dispositivos de almacenamiento masivo y unidades de CD/DVD para proteger el equipo contra amenazas de la seguridad informática, que pueden ocurrir en el proceso de intercambio de archivos con unidades flash u otro tipo de dispositivos externos conectados mediante USB. Los dispositivos de almacenamiento masivo son dispositivos externos que pueden conectarse a un equipo para copiar o almacenar archivos.

Kaspersky Embedded Systems Security controla las siguientes conexiones de dispositivos externos de USB:

- Unidades flash conectadas mediante USB
- Unidades CD-ROM
- Unidades de discos flexibles conectadas mediante USB
- Dispositivos móviles MTP conectados mediante USB

Kaspersky Embedded Systems Security le informa sobre todos los dispositivos conectados mediante USB con el correspondiente evento en los registros de tareas y eventos. Los detalles de los eventos incluyen el tipo de dispositivo y la ruta de acceso de la conexión. Cuando se inicia la tarea de control de dispositivos, Kaspersky Embedded Systems Security comprueba y enumera todos los dispositivos conectados mediante USB. Puede configurar las notificaciones en la sección de configuración de notificaciones de Kaspersky Security Center.

La tarea Control de dispositivos supervisa todos los intentos de conexiones de dispositivos externos a un equipo protegido mediante USB y bloquea la conexión si no hay reglas de autorización para tales dispositivos. Después de que se bloquea la conexión, el dispositivo no está disponible.

La aplicación asigna uno de los siguientes estados a cada dispositivo de almacenamiento masivo conectado:

- *Confiable*. Dispositivo para el cual desea permitir el intercambio de archivos. Después de la generación de la lista de reglas, el valor de la *Ruta de acceso a la instancia del dispositivo* se incluye en el área de uso para al menos una regla.
- *Dudoso*. Dispositivo para el cual desea restringir el intercambio de archivos. La ruta de acceso a la instancia del dispositivo no se incluye en ninguna área de aplicación de las reglas de autorización.

Puede crear reglas de autorización para que el dispositivo externo autorice el intercambio de datos a través del uso de la tarea de Generador de reglas para Control de dispositivos. También puede ampliar el área de aplicación de las reglas ya especificadas. No puede crear reglas de autorización manualmente.

Kaspersky Embedded Systems Security identifica dispositivos de almacenamiento masivo registrados en el sistema con el valor Ruta de acceso a la instancia del dispositivo. La ruta de acceso a la instancia del dispositivo es una función predeterminada especificada únicamente para cada dispositivo externo. El valor de la ruta de acceso a la instancia del dispositivo se especifica para cada dispositivo externo en sus propiedades de Windows, y Kaspersky Embedded Systems Security lo determina automáticamente durante la generación de reglas.

La tarea de Control de dispositivos puede funcionar en dos modos:

- **Activar**. Kaspersky Embedded Systems Security aplica reglas para controlar la conexión de unidades flash y otros dispositivos externos, y autoriza o bloquea el uso de todos los dispositivos según el principio de denegación predeterminada y las reglas de autorización especificadas. Se autoriza el uso de dispositivos externos de confianza. El uso de dispositivos externos dudosos sea bloquea de forma predeterminada.

  Si un dispositivo externo que se considera dudoso se conecta a un equipo protegido antes de que la tarea Control de dispositivos se ejecute en modo **Activar**, la aplicación no bloquea el dispositivo. Se recomienda desconectar el dispositivo dudoso manualmente o reiniciar el equipo. De lo contrario, el principio Denegar por defecto no se aplicará al dispositivo.

- **Solo estadísticas**. Kaspersky Embedded Systems Security no controla la conexión de unidades flash ni otros dispositivos externos, sino que solo registra la información sobre la conexión y el registro de dispositivos externos en un equipo protegido y sobre las reglas de autorización de Control de dispositivos que activan los dispositivos conectados. Se autoriza el uso de todos los dispositivos externos. Este modo está configurado de forma predeterminada.

  Puede aplicar este modo para la generación de reglas según la información sobre bloqueos registrada durante la ejecución de la tarea (consulte la sección Llenado de la lista de reglas según los eventos de la tarea de Control de dispositivos, en la página 358).

Acerca de las Reglas de Control de dispositivos

Las reglas se generan de manera única para cada dispositivo conectado en ese momento o que se haya conectado alguna vez a un equipo protegido si la información sobre este dispositivo se almacena en el registro del sistema.

Para generar reglas de autorización para el control de dispositivos, puede realizar lo siguiente:

- Aplicar la tarea de Generador de reglas para Control de dispositivos (consulte la sección “Acerca del generador de reglas para la tarea Control de dispositivos”, en la página 341).
- Ejecute la tarea Control de dispositivos en el modo Solo estadísticas (consulte la sección “Llenado de la lista de reglas en eventos de tareas de Control de dispositivos”, en la página 358).
- Aplique la información del sistema sobre dispositivos conectados anteriormente (consulte la sección “Cómo agregar una regla de autorización para uno o varios dispositivos externos”, en la página 358).
- Ampliar el área de aplicación de las reglas ya especificadas (consulte la sección “Ampliación del área de aplicación de las reglas de control de dispositivos”, en la página 360).

Kaspersky Embedded Systems Security admite una cantidad máxima cantidad de 3072 reglas de control de dispositivos.

Las reglas de control de dispositivos se describen a continuación.

Tipo de regla

El tipo de regla siempre es *de autorización*. De forma predeterminada, la tarea Control de dispositivos bloquea todas las conexiones de unidades flash y de otros dispositivos externos si estos dispositivos no se incluyen en ninguna área de aplicación de las reglas de autorización.

Criterio de activación y área de aplicación de la regla

Las reglas de Control de dispositivos identifican las unidades flash y otros dispositivos externos según la *Ruta de acceso a la instancia del dispositivo*. La ruta de acceso a la instancia del dispositivo es un criterio único que el sistema asigna a un dispositivo cuando este se conecta y se registra como dispositivo de almacenamiento masivo o unidad de CD/DVD (por ejemplo, IDE o SCSI).

Kaspersky Embedded Systems Security controla la conexión de la unidad de CD/DVD sin tener en cuenta el bus usado para la conexión. Al montar el dispositivo mediante USB, el sistema operativo registra dos valores de ruta de acceso a la instancia del dispositivo: uno para el dispositivo de almacenamiento masivo y otro para la unidad de CD/DVD (por ejemplo, IDE o SCSI). Para conectar estos dispositivos correctamente, se deben configurar las reglas de autorización para cada valor de ruta de acceso a la instancia.

Kaspersky Embedded Systems Security define automáticamente la ruta de acceso a la instancia del dispositivo y analiza el valor obtenido en los elementos siguientes:

- fabricante del dispositivo (VID);
- tipo de controlador del dispositivo (PID);
- número de serie del dispositivo.

No puede configurar la ruta de acceso a la instancia del dispositivo manualmente. Los criterios de activación de la

regla de autorización definen el área de aplicación de la regla. De forma predeterminada, el área de aplicación de las reglas creadas recientemente incluye un dispositivo inicial, según las propiedades sobre quien Kaspersky Embedded Systems Security había generado la regla. Puede configurar los valores en la configuración de la regla creada usando una máscara para ampliar el área de aplicación de la regla (consulte la sección “Expansión del área de aplicación de las reglas de Control de dispositivos”, en la página 360).

Valores iniciales del dispositivo

Propiedades del dispositivo que Kaspersky Embedded Systems Security usó para la generación de reglas de autorización y que se muestran en el Administrador de dispositivos de Windows para cada dispositivo conectado.

Los valores iniciales del dispositivo contienen la siguiente información:

- **Ruta de acceso a la instancia del dispositivo**. Según esta propiedad, Kaspersky Embedded Systems Security define los criterios de activación de la regla y completa los campos siguientes: **Fabricante (VID)**, **Tipo de controlador (PID)**, **Número de serie** en la sección **Área de aplicación de la regla** de la ventana **Propiedades de la regla**.
- **Nombre descriptivo**. Nombre del dispositivo que está configurado en las propiedades del dispositivo por su fabricante.

Kaspersky Embedded Systems Security automáticamente define valores iniciales del dispositivo cuando la regla se está generando. Más tarde, puede usar estos valores para reconocer el dispositivo que se utilizó como base para la generación de la regla. Los valores iniciales del dispositivo no están disponibles para su modificación.

Descripción

Puede agregar información adicional para cada regla de control de dispositivos creada en el campo **Descripción**; por ejemplo, puede anotar el nombre de la unidad flash conectada o definir a su propietario. La descripción se muestra en un gráfico correspondiente en la ventana **Reglas de Control de dispositivos**.

La descripción y los valores iniciales del dispositivo no tienen permitida la activación de reglas y se asignan solo para simplificar la identificación del dispositivo por parte del usuario.

Acerca del llenado de listas de reglas de Control de dispositivos

Puede importar reglas de autorización de control de dispositivos de los archivos XML que se generaron automáticamente durante la ejecución de las tareas de Control de dispositivos o de Generador de reglas para Control de dispositivos.

De forma predeterminada, Kaspersky Embedded Systems Security restringe las conexiones de cualquier unidad flash y otros dispositivos externos si no se incluyen en el área de aplicación de las reglas de control de dispositivos especificadas.

Tabla 49. Objetivos y escenarios para la generación de listas de Reglas de Control de dispositivos

Escenario de generación de reglas	Objetivo
Tarea de Generador de reglas para Control de dispositivos	• Agregue reglas de autorización de dispositivos de confianza conectados anteriormente antes del primer inicio de la tarea de Control de dispositivos. • Genere listas de reglas para dispositivos de confianza en la red de equipos protegidos.
Generación de reglas según datos de sistema	Agregue reglas de autorización para uno o varios dispositivos conectados recientemente.
La tarea Control de dispositivos en el modo **Solo estadísticas**	Genere reglas de autorización para un gran número de dispositivos de confianza.

Uso de la regla Generador de reglas para Control de dispositivos

El archivo XML, generado después de la finalización de la tarea de Generador de reglas para Control de dispositivos, contiene reglas de autorización para las unidades flash y otros dispositivos externos cuyos datos se han almacenado en un registro del sistema.

Durante la ejecución de la tarea, Kaspersky Embedded Systems Security recibe datos del sistema sobre todos los dispositivos de almacenamiento masivo que se hayan conectado alguna vez o estén conectados en ese momento a un equipo protegido y genera la lista de reglas de autorización según los datos del sistema para los dispositivos detectados. Después de la finalización de la tarea, la aplicación crea el archivo XML en la carpeta que se ubica en la ruta especificada en la configuración de la tarea. Puede configurar la importación automática de las reglas generadas en la lista de reglas para la tarea de Control de dispositivos.

Este escenario se recomienda para generar la lista de reglas de autorización antes del primer inicio de la tarea de Control de dispositivos, de modo que las reglas de autorización generadas abarquen todos los dispositivos externos de confianza que se utilicen en un equipo protegido.

Uso de datos de sistema sobre todos los dispositivos conectados

Durante la ejecución de la tarea, Kaspersky Embedded Systems Security recibe datos del sistema sobre todos los dispositivos externos que se hayan conectado alguna vez o estén conectados en ese momento a un equipo protegido y muestra los dispositivos detectados en la lista de la ventana **Generar reglas basadas en información del sistema**.

Para cada dispositivo detectado, Kaspersky Embedded Systems Security analiza los valores de fabricante (VID), el tipo de controlador (PID), el nombre descriptivo, el número de serie y la ruta de acceso a la instancia del dispositivo. Puede generar reglas de autorización para cualquier dispositivo de almacenamiento masivo cuyos datos se hayan almacenado en el sistema, y agregar directamente reglas creadas recientemente a la lista de las Reglas de Control de dispositivos.

Este escenario se recomienda para renovar una lista de reglas ya especificada cuando es necesario confiar en una cantidad pequeña de dispositivos de almacenamiento masivo nuevos.

Kaspersky Embedded Systems Security no obtiene el acceso a datos del sistema sobre los dispositivos móviles conectados mediante MTP. No puede generar reglas de autorización para dispositivos móviles conectados a MTP.

Uso de la tarea Control de dispositivos en el modo Solo estadísticas

El archivo XML recibido después de la finalización de la tarea de Control de dispositivos en el modo **Solo estadísticas** se genera según el registro de tareas.

Durante la ejecución de la tarea, Kaspersky Embedded Systems Security registra información sobre todas las conexiones de unidades flash y otros dispositivos de almacenamiento masivo a un equipo protegido. Puede generar reglas de autorización según eventos de la tarea y exportarlas a un archivo XML. Antes de iniciar la tarea en el modo **Solo estadísticas**, se recomienda configurar el periodo de ejecución de la tarea, de modo que, durante el periodo especificado, se realicen todas las conexiones de dispositivos externos posibles con un equipo protegido.

Este escenario se recomienda para renovar una lista de reglas ya generada si se debe autorizar un gran número de dispositivos externos nuevos.

Si la generación de la lista de reglas según este escenario se realiza en una máquina modelo, puede aplicar una lista de reglas de autorización generadas al configurar la tarea de Control de dispositivos mediante Kaspersky Security Center. De esta manera, podrá autorizar el uso de dispositivos externos conectados a una máquina modelo en todos los equipos, incluidos los de una red protegida.

Acerca de la tarea de Generador de reglas para Control de dispositivos

La tarea de Generador de reglas para Control de dispositivos puede crear automáticamente una lista de reglas de autorización para unidades flash conectadas y otros dispositivos de almacenamiento masivo según los datos de sistema sobre todos los dispositivos externos que se hayan conectado alguna vez a un equipo protegido.

> Kaspersky Embedded Systems Security no obtiene el acceso a datos del sistema sobre los dispositivos móviles conectados mediante MTP. No puede generar reglas de autorización para dispositivos móviles conectados a MTP.

Después de la finalización de la tarea, Kaspersky Embedded Systems Security crea un archivo XML de configuración que contiene la lista de reglas de autorización para todos los dispositivos externos detectados, o directamente agrega reglas generadas en la tarea de Control de dispositivos según la configuración del Generador de reglas para Control de dispositivos. La aplicación autorizará posteriormente los dispositivos para los cuales se generaron reglas de autorización automáticamente.

Las reglas generadas y agregadas en la tarea se muestran en la ventana **Reglas de Control de dispositivos**.

Escenarios de generación de reglas de Control de dispositivos

Puede generar reglas (consulte la sección “Generación de reglas de Control de dispositivos para todos los equipos mediante Kaspersky Security Center”, en la página 347) basadas en datos de Windows sobre todos los dispositivos de almacenamiento masivo que se han conectado históricamente o están conectados actualmente según tres escenarios:

- Con la tarea de grupo de Generador de reglas para Control de dispositivos. Use este escenario durante el proceso de generación de reglas para tener en cuenta todos los dispositivos de almacenamiento masivo

que alguna vez se hayan conectado y que estén registrados por los sistemas en todos los equipos de red.

- Usar la opción **Generar reglas basadas en datos del sistema**. Use este escenario durante el proceso de generación de reglas para tener en cuenta todos los dispositivos de almacenamiento masivo que alguna vez se hayan conectado y que estén registrados por el sistema de un equipo con la Consola de administración de Kaspersky Security Center.
- Usar **Generar reglas basadas en los dispositivos conectados** en la ventana **Reglas de Control de dispositivos** y la configuración de la tarea del Generador de reglas para Control de dispositivos. Use este método si desea solo considerar datos sobre dispositivos actualmente conectados al equipo protegido al generar el permiso de reglas.

Kaspersky Embedded Systems Security no obtiene el acceso a datos del sistema sobre los dispositivos móviles conectados mediante MTP. No puede generar reglas de autorización para dispositivos móviles de confianza conectados a MTP con escenarios para el llenado de listas de reglas sobre la base de datos del sistema sobre todos los dispositivos conectados.

Configuración predeterminada de la tarea de Control de dispositivos

De forma predeterminada, la tarea de Control de dispositivos tiene la configuración descrita en la tabla a continuación. Puede cambiar los valores de esta configuración.

Tabla 50. Configuración de la tarea de control de dispositivos

Configuración	Valor predeterminado	Descripción
Modo de la tarea	**Solo estadísticas**	La tarea registra información sobre dispositivos externos que se bloquearon o se autorizaron según las reglas especificadas. Los dispositivos externos, en realidad, no se bloquean. Puede seleccionar el modo **Activar** para que la protección del equipo bloquee realmente el uso de dispositivos externos.
Permitir el uso de todos los dispositivos de almacenamiento masivo cuando la tarea Control de dispositivos no se esté ejecutando	No aplicado	Kaspersky Embedded Systems Security bloquea el uso de dispositivos externos sin tener en cuenta el estado de la tarea de Control de dispositivos. Esto proporciona el nivel de protección máximo contra las amenazas de seguridad informática que surgen al intercambiar archivos con dispositivos externos. Puede ajustar el parámetro de modo que Kaspersky Embedded Systems Security autorice el uso de todos los dispositivos externos cuando la tarea de Control de dispositivos no está en ejecución.
Programación de inicio de tareas	La primera ejecución no está programada.	La tarea de Control de dispositivos no se inicia automáticamente al inicio de Kaspersky Embedded Systems Security. Puede configurar la programación de inicio de tareas.

Tabla 51. Configuración predeterminada de la tarea de Generador de reglas para Control de dispositivos

Configuración	Valor predeterminado	Descripción
Modo de la tarea	**Tener en cuenta los datos del sistema sobre todas las unidades de almacenamiento masivo que se hayan conectado alguna vez**	El modo de operación de la tarea. Puede seleccionar el modo de tarea **Considerar solamente los dispositivos de almacenamiento masivo conectados actualmente**.
Acciones después de la finalización de la tarea	Las reglas de autorización se agregan a la lista de reglas de Control de dispositivos, las reglas nuevas se fusionan con las existentes y las reglas duplicadas se eliminan.	Puede agregar reglas a las existentes sin fusionarlas y sin eliminar las reglas duplicadas; reemplazar las reglas existentes con reglas de autorización nuevas; o configurar la exportación de reglas de autorización a un archivo.
Programación de inicio de tareas	La primera ejecución no está programada.	La tarea de Generador de reglas para Control de dispositivos no se inicia automáticamente al inicio de Kaspersky Embedded Systems Security. Puede iniciar la tarea manualmente o configurar un inicio programado.

Gestión del Control de dispositivos a través del Complemento de administración

En esta sección, aprenda cómo navegar a través de la interfaz del Complemento de administración y gestionar las conexiones del cualquier dispositivo de almacenamiento masivo a todos los equipos en la red generando listas de reglas a través de Kaspersky Security Center para los grupos de equipos.

En esta sección

Navegación

Sepa cómo navegar a la configuración de la tarea requerida a través de la interfaz.

En esta sección

Cómo abrir la configuración de la directiva para la tarea de Control de dispositivos

► *Para abrir la configuración de la tarea de Control de dispositivos a través de la directiva de Kaspersky Security Center:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas.**
4. Haga doble clic en el nombre de la directiva que desea configurar.

5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Control de actividad local**.
6. Haga clic en el botón **Configurar** en la subsección **Control de dispositivos**.

   Se abre la ventana **Control de dispositivos**.
7. Configure la directiva según sea necesario.

Cómo abrir la lista de reglas de Control de dispositivos

► *Para abrir la lista de reglas de Control de dispositivos a través de Kaspersky Security Center:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas.**
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Control de actividad local**.
6. Haga clic en el botón **Configurar** en la subsección **Control de dispositivos**.

   Se abre la ventana **Control de dispositivos**.
7. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

   Se abre la ventana **Reglas de Control de dispositivos**.
8. Configure la directiva según sea necesario.

Cómo abrir las propiedades y el asistente de la tarea de Generador de reglas para Control de dispositivos

► *Para iniciar la creación de una tarea de Generador de reglas para Control de dispositivos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Tareas**.
4. Haga clic en el botón **Crear una tarea**.

   Se abre la ventana **Nuevo asistente de tarea**.
5. Seleccione la tarea **Generador de reglas para Control de dispositivos**.
6. Haga clic en **Siguiente**.

   Se abre la ventana **Configuración**.

► *Para configurar la tarea existente de Generador de reglas para Control de dispositivos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.

3. Seleccione la pestaña **Tareas**.
4. Haga doble clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

   Se abre la ventana **Propiedades: Generador de reglas para Control de dispositivos**.

Consulte la sección Configuración de la tarea Generador de reglas para Control de dispositivos para obtener más información sobre la configuración de la tarea.

Configuración de la tarea de Control de dispositivos

► *Para ajustar la configuración de la tarea Control de dispositivos:*

1. Abra la ventana **Control de dispositivos** (consulte la sección "Cómo abrir la configuración de la directiva para la tarea de Control de dispositivos" en la página 344).
2. En la pestaña **General**, configure la siguiente configuración de tarea:
   - En la sección **Modo de la tarea**, seleccione uno de los modos de la tarea:
     - **Activar**.

       Kaspersky Embedded Systems Security aplica reglas para controlar la conexión de unidades flash y otros dispositivos externos, y autoriza o bloquea el uso de todos los dispositivos según el principio Denegar por defecto y las reglas de autorización especificadas. Se autoriza el uso de dispositivos externos de confianza. El uso de dispositivos externos dudosos sea bloquea de forma predeterminada.

     Si un dispositivo externo que se considera dudoso se conecta a un equipo protegido antes de que la tarea Control de dispositivos se ejecute en modo Activo, la aplicación no bloquea el dispositivo. Se recomienda desconectar el dispositivo dudoso manualmente o reiniciar el equipo. De lo contrario, el principio Denegar por defecto no se aplicará al dispositivo.

     - **Solo estadísticas**.

       Kaspersky Embedded Systems Security no controla la conexión de unidades flash ni otros dispositivos externos, sino que solo registra la información sobre la conexión y el registro de dispositivos externos en un equipo protegido y sobre las reglas de autorización de Control de dispositivos que activan los dispositivos conectados. Se autoriza el uso de todos los dispositivos externos. Este modo está configurado de forma predeterminada.
   - Seleccione o desactive la casilla de verificación **Permitir el uso de todos los dispositivos de almacenamiento masivo cuando la tarea Control de dispositivos no se esté ejecutando**.

     La casilla de verificación permite autorizar o bloquear el uso de dispositivos de almacenamiento masivo cuando la tarea de Control de dispositivos no se está ejecutando.

     Si la casilla está seleccionada y la tarea Control de dispositivos no se está ejecutando, Kaspersky Embedded Systems Security permite usar cualquier dispositivo de almacenamiento en un equipo protegido.

     Si la casilla de verificación está desactivada, la aplicación bloquea el uso de dispositivos de almacenamiento masivo dudosos en un equipo protegido en los siguientes casos: la tarea de Control de dispositivos no se está ejecutando o el servicio de Kaspersky Security se ha detenido. Esta opción se recomienda para maximizar el nivel de

protección contra las amenazas de seguridad informática que surgen al intercambiar archivos con dispositivos externos.

De forma predeterminada, la casilla está desactivada.

3. Haga clic el botón de la lista **Lista de reglas** para modificar la lista de reglas del Control de dispositivos (consulte la sección "Configuración de reglas de Control de dispositivos mediante Kaspersky Security Center" en la página 349).
4. De ser necesario, configure la programación de inicio de tareas en la pestaña **Administración de la tarea**.
5. Haga clic en **Aceptar**.

Kaspersky Embedded Systems Security aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de tareas.

Generación de reglas de Control de dispositivos para todos los equipos mediante Kaspersky Security Center

Puede crear listas de reglas de Control de dispositivos usando tareas de Kaspersky Security Center para todos los equipos y los grupos de equipos en la red corporativa a la vez.

Puede crear listas de reglas de Control de dispositivos del lado de Kaspersky Security Center de las siguientes maneras:

- Con la tarea de grupo de Generador de reglas para Control de dispositivos.

  Según este escenario, la tarea de grupo genera listas de reglas, basadas en datos del sistema de cada equipo, sobre todos los dispositivos de almacenamiento masivo que alguna vez se hayan conectado a equipos protegidos. La tarea también autoriza todos los dispositivos de almacenamiento masivo que están conectados en el momento de ejecución de la tarea. Después de la finalización de la tarea de grupo, Kaspersky Embedded Systems Security genera listas de reglas de autorización para todos los dispositivos de almacenamiento masivo registrados en la red y guarda estas listas en un archivo XML en una carpeta especificada. Luego, puede importar manualmente las reglas generadas en la configuración de la tarea de control de dispositivos. A diferencia de una tarea en un equipo local, la directiva no permite configurar la adición automática de las reglas creadas a la lista de reglas de Control de dispositivos cuando se completa la tarea de grupo del Generador de reglas para Control de dispositivos.

  Este escenario se recomienda para generar la lista de reglas de autorización antes del primer inicio de la tarea de Control de dispositivos en el modo de aplicación de reglas **Activa**.

  > Antes de usar la directiva de Control de dispositivos en la red, asegúrese de que todos los equipos protegidos puedan acceder a una carpeta de red compartida. Si la directiva de la organización no asegura el uso de una carpeta de red compartida en la red, se recomienda iniciar la tarea Generador de reglas para Control de dispositivos para las reglas de Control del equipo en el grupo de equipos de prueba o en una máquina modelo.

- Según un informe sobre los eventos de tareas generadas en Kaspersky Security Center para la operación de la tarea de Control de dispositivos en el modo **Solo estadísticas**.

  Según este escenario, Kaspersky Embedded Systems Security no restringe las conexiones de dispositivos de almacenamiento masivo, sino que registra información sobre todas las conexiones de dispositivos y registro de dispositivos de almacenamiento masivo en todos los equipos de red durante la tarea de Control de dispositivos que se ejecutan en el modo **Solo estadísticas**. La información registrada puede

encontrarse en la pestaña **Eventos** del área de trabajo del nodo **Servidor de administración** del Kaspersky Security Center. Kaspersky Security Center genera una lista unificada de eventos de autorización y restricción de dispositivos de almacenamiento masivo según el registro de tareas.

Debe configurar el periodo de la tarea en ejecución de modo que todas las conexiones de dispositivos de almacenamiento masivo se realicen durante el periodo establecido. Luego, a medida que las reglas se agreguen a la tarea de Control de dispositivos, puede importar datos en conexiones de dispositivos desde el archivo de informe de eventos de Kaspersky Security Center guardado (en formato TXT) y generar reglas de autorización de Control de dispositivos para tales dispositivos según estos datos. El tipo de eventos, en los que se basa un registro importado, no influye en el tipo de reglas generado; solo se generan reglas de autorización.

Este escenario se recomienda para agregar reglas de autorización para un gran número de dispositivos de almacenamiento masivo nuevos, así como para generar reglas para los dispositivos móviles de confianza conectados a MTP.

- Basándose en los datos del sistema acerca de dispositivos de almacenamiento masivo conectados (con la opción **Generar reglas basadas en datos del sistema** en la configuración de la tarea de Control de dispositivos).

  Según este escenario, Kaspersky Embedded Systems Security genera reglas de autorización para los dispositivos de almacenamiento masivo que alguna vez se hayan conectado o que estén conectados en ese momento a un equipo con Kaspersky Security Center instalado.

  Este escenario se recomienda para generar reglas para un número pequeño de dispositivos de almacenamiento masivo nuevos en los que desee confiar en todos los equipos en la red.

- Basándose en los datos sobre los dispositivos actualmente conectados (con **Generar reglas basadas en los dispositivos conectados**).

  En esta situación, Kaspersky Embedded Systems Security genera reglas de autorización solo para dispositivos actualmente conectados. Puede seleccionar uno o varios dispositivos para los que desea generar reglas de autorización.

  > Kaspersky Embedded Systems Security no obtiene el acceso a datos del sistema sobre los dispositivos móviles conectados mediante MTP. No puede generar reglas de autorización para dispositivos móviles de confianza conectados a MTP con escenarios para el llenado de listas de reglas sobre la base de datos del sistema sobre todos los dispositivos conectados.

Configuración de la tarea Generador de reglas para Control de dispositivos

► *Para configurar la tarea de Generador de reglas para Control de dispositivos, haga lo siguiente:*

1. Abra la ventana **Propiedades:** Ventana **Generador de reglas para Control de dispositivos** (consulta la sección "**Cómo abrir las propiedades y el asistente de la tarea de Generador de reglas para Control de dispositivos**" en la página 345).
2. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.

   > Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

3. En la sección **Configuración**, puede establecer la siguiente configuración:

   - Seleccione el modo de operación: considere los datos de sistema acerca de todos los dispositivos de almacenamiento masivo que se hayan conectado alguna vez o solo considere los depósitos masivos

actualmente conectados.

- Ajuste la configuración para archivos de configuración con listas de reglas de autorización que Kaspersky Embedded Systems Security crea después de la finalización de la tarea.

4. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
5. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para la ejecución de la tarea.
6. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones del área de la tarea**.

   Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

7. En la ventana **Propiedades: <Nombre de la tarea>**, haga clic en **Aceptar**.

   Se guardan las opciones de las tareas de grupo recientemente configuradas.

Configuración de reglas de Control de dispositivos mediante Kaspersky Security Center

Aprenda cómo generar una lista de reglas según distintos criterios o crear manualmente las reglas de autorización o denegación utilizando la tarea de Control de dispositivos.

En esta sección

Creación de reglas de autorización a partir de datos de sistema en una directiva de Kaspersky Security Center

► *Para especificar reglas de autorización utilizando la opción **Generar reglas basadas en datos del sistema** en la tarea de Control de dispositivos:*

1. Si es necesario, conecte un dispositivo de almacenamiento masivo nuevo que desee que sea de confianza para un equipo con la Consola de administración de Kaspersky Security Center instalada.
2. Abra la ventana **Reglas de Control de dispositivos** (consulte la sección "Cómo abrir la lista de reglas de Control de dispositivos" en la página 345).
3. Haga clic en el botón **Agregar** y, en el menú contextual que se abre, seleccione la opción **Generar reglas basadas en datos del sistema**.
4. Seleccione el principio para agregar las reglas de autorización a la lista de reglas de Control de

dispositivos creadas anteriormente:

- Seleccione un dispositivo de la lista de dispositivos que figura en la ventana **Generar reglas basadas en información del sistema**.
- Haga clic en **Agregar reglas para los dispositivos seleccionados**.

5. Haga clic en el botón **Guardar** en la ventana **Reglas de Control de dispositivos**.

La lista de reglas en la tarea de Control de dispositivos se completará con reglas nuevas generadas según un dato de sistema del equipo con la Consola de administración de Kaspersky Security Center instalada.

Generación de reglas para dispositivos conectados

► *Para especificar reglas de autorización con la opción **Generar reglas basadas en los dispositivos conectados** en la tarea de Control de dispositivos:*

1. Abra la ventana **Reglas de Control de dispositivos** (consulte la sección "**Cómo abrir la lista de reglas de Control de dispositivos**" en la página 345).
2. Haga clic en el botón **Agregar** y, en el menú contextual, seleccione **Generar reglas basadas en los dispositivos conectados**.

   Se abre la ventana **Generar reglas basadas en información del sistema**.
3. En la lista de dispositivos detectados conectados al equipo protegido, seleccione los dispositivos para los cuales desea generar reglas de autorización.
4. Haga clic en el botón **Agregar reglas para los dispositivos seleccionados**.
5. Haga clic en el botón **Guardar** en la ventana **Reglas de Control de dispositivos**.

La lista de reglas en la tarea de Control de dispositivos se completará con reglas nuevas generadas según un dato de sistema del equipo con la Consola de administración de Kaspersky Security Center instalada.

Importación de reglas desde el informe de Kaspersky Security Center sobre dispositivos bloqueados

Puede importar datos sobre conexiones de dispositivos bloqueados desde el informe generado en Kaspersky Security Center después de la finalización de la tarea de Control de dispositivos en el modo **Solo estadísticas** (consulte la sección "Configuración de la tarea de Control de dispositivos" en la página 346) y usar estos datos para generar una lista de reglas de autorización de Control de dispositivos en la directiva configurada.

Al generar el informe sobre eventos que ocurren durante la tarea de Control de dispositivos, puede hacer un seguimiento de los dispositivos cuya conexión se restringe.

► *Para especificar reglas de autorización para la conexión de dispositivos para un grupo de equipos según el informe de Kaspersky Security Center sobre dispositivos bloqueados:*

1. En las propiedades de la directiva, en la sección **Notificación de eventos**, asegúrese de que:
   - Para el nivel de importancia de **Eventos críticos** , el período para almacenar el registro de tareas para el evento *Almacenamiento masivo restringido* supera el período planeado de la operación en el modo **Solo estadísticas** (el valor predeterminado es 30 días).
   - Para el nivel de importancia de **Advertencia**, el período de tiempo para almacenar el registro de tareas para el evento *Solo estadísticas: almacenamiento masivo dudoso detectado* supera el período planeado de operación de la tarea en el modo **Solo estadísticas** (el valor predeterminado es 30 días).

   Cuando el periodo para almacenar eventos se agota, la información sobre los eventos registrados se elimina y no se refleja en el archivo del informe. Antes de ejecutar la tarea de Control de dispositivos en el modo **Solo estadísticas**, asegúrese de que el tiempo de ejecución de la tarea no supere el tiempo de almacenamiento configurado para los eventos especificados.
2. Inicie la tarea de Control de dispositivos en el modo **Solo estadísticas**. En el espacio de trabajo del nodo **Servidor de administración** en Kaspersky Security Center**,** seleccione la pestaña **Eventos**. Haga clic en el botón **Crear una selección** y cree una selección de eventos según el criterio *Almacenamiento masivo dudoso* para ver los dispositivos cuyas conexiones serán restringidas por la tarea de Control de dispositivos. En el panel de detalles de la selección, haga clic en el vínculo **Exportar eventos a archivo** para guardar el informe sobre conexiones restringidas a un archivo TXT.

   Antes de importar y aplicar el informe generado en una directiva, asegúrese de que el informe solo contenga datos de los dispositivos cuya conexión desea autorizar.
3. Importe datos sobre conexiones de dispositivos restringidos a la tarea de Control de dispositivos:
   a. Abra la ventana **Reglas de Control de dispositivos** (consulte la sección "Cómo abrir la lista de reglas de Control de dispositivos" en la página 345).
   b. Haga clic en el botón **Agregar** y, en el menú contextual del botón, seleccione **Importar datos sobre dispositivos bloqueados del informe de Kaspersky Security Center**.
   c. Seleccione el principio para agregar reglas desde la lista creada sobre la base del informe de Kaspersky Security Center a la lista de reglas de Control de dispositivos configuradas anteriormente:
      - **Agregar a reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
      - **Reemplazar reglas existentes** si desea reemplazar las reglas existentes con las reglas importadas.
      - **Combinar con reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.
   d. En la ventana estándar de Microsoft Windows que se abre, seleccione el archivo TXT al cual se exportaron los eventos del informe sobre dispositivos restringidos.
   e. Haga clic en el botón **Guardar** en la ventana **Reglas de Control de dispositivos**.
4. Haga clic en **Aceptar** en la ventana **Control de dispositivos**.

Las reglas creadas sobre la base del informe de Kaspersky Security Center sobre los dispositivos restringidos se agregan a la lista de reglas de Control de dispositivos.

Creación de reglas con la tarea Generador de reglas para Control de dispositivos

► *Para especificar reglas de control de dispositivos para un grupo de equipos mediante la tarea de Generador de reglas para Control de dispositivos:*

1. Abra la ventana **Configuración** en el **Nuevo asistente de tarea** (consulte la sección "**Cómo abrir las propiedades y el asistente de la tarea de Generador de reglas para Control de dispositivos**" en la página 345).
2. Configure lo siguiente:
   - En la sección **Modo**:
     - **Tener en cuenta los datos del sistema sobre todas las unidades de almacenamiento masivo que se hayan conectado alguna vez**.
     - **Tener en cuenta solo las unidades de almacenamiento masivo conectadas actualmente**.
   - En la sección **Después de completada la tarea**:
     - **Agregar reglas de autorización a la lista de reglas de Control de dispositivos**.

       La casilla de verificación habilita o deshabilita la adición de reglas de autorización recientemente generadas a la lista de reglas de Control de dispositivos. La lista de reglas de Control de dispositivos se muestra cuando hace clic en el vínculo **Reglas de Control de dispositivos** en el panel de detalles del nodo **Control de dispositivos**.

       Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security agrega las reglas generadas por la tarea de Generador de reglas para Control de dispositivos a la lista de reglas de Control de dispositivos, según el principio de adición seleccionado.

       Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security no agrega las reglas de autorización recientemente generadas a la lista de reglas de Control de dispositivos. Las reglas generadas solo se exportan a un archivo.

       De forma predeterminada, la casilla está activada.

       La casilla de verificación no se puede seleccionar si la casilla de verificación **Exportar reglas de autorización a archivo** no está seleccionada.

     - **Principio de adición**.

       La lista desplegable se utiliza para especificar el método utilizado para agregar las reglas de autorización recientemente generadas a la lista de reglas de Control de inicio de aplicaciones.

       - **Agregar a reglas existentes**. Las reglas se agregan a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
       - **Reemplazar reglas existentes**. Las reglas reemplazan a las reglas existentes en la lista.
       - **Combinar con reglas existentes**. Las reglas se agregan a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

       De forma predeterminada, está seleccionado el método **Combinar con reglas existentes**.

     - **Exportar reglas de autorización a archivo**.

       La casilla de verificación habilita o deshabilita la exportación de reglas de autorización

desde Control de dispositivos a un archivo.

Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security exporta las reglas de autorización al archivo especificado en el campo a continuación cuando finaliza la tarea de Generador de reglas para Control de dispositivos.

Si esta casilla se desactiva, la aplicación no exporta las reglas de autorización generadas a un archivo cuando finaliza la tarea del Generador de reglas para Control de dispositivos. En cambio, solo las agrega a la lista de reglas de Control de dispositivos.

De forma predeterminada, la casilla está desactivada.

La casilla de verificación no se puede seleccionar si la casilla de verificación **Agregar reglas de autorización a la lista de reglas de Control de dispositivos** no se seleccionó.

- **Agregar detalles del equipo al nombre del archivo**.

  La casilla de verificación habilita o deshabilita la adición de información sobre el equipo protegido al nombre del archivo al que se exportarán las reglas de autorización.

  Si esta casilla de verificación está seleccionada, la aplicación agrega el nombre del equipo protegido y la fecha y hora de creación del archivo al nombre del archivo de exportación.

  Si la casilla de verificación está desactivada, la aplicación no agrega información sobre el equipo protegido al nombre del archivo de exportación.

  De forma predeterminada, la casilla está activada.

3. Haga clic en **Siguiente**.
4. En la ventana **Programación**, configure los ajustes del inicio de la tarea programada.
5. Haga clic en **Siguiente**.
6. En la ventana **Seleccionar una cuenta para ejecutar la tarea**, especifique la cuenta que desea utilizar.
7. Haga clic en **Siguiente**.
8. Defina el nombre de la tarea.
9. Haga clic en **Siguiente**.

   El nombre de la tarea no debe tener más de 100 caracteres y no puede contener los siguientes símbolos:
   " * < > & \ : |

   Se abre la ventana **Finalizar creación de la tarea**.
10. Puede ejecutar la tarea opcionalmente después de que el Asistente finalice, seleccionando la casilla **Ejecutar tarea después de que finalice el asistente**.
11. Haga clic en **Finalizar** para terminar de crear la tarea.
12. En la pestaña **Tareas** en el espacio de trabajo del grupo de equipos configurados, en la lista de tareas de grupo, seleccione el Generador de reglas para Control de dispositivos que creó.
13. Haga clic en el botón **Inicio** para iniciar la tarea.

    Cuando la tarea se completa, las listas de reglas de autorización generadas automáticamente se guardan en una carpeta compartida en archivos XML.

Antes de usar la directiva de Control de dispositivos en la red, asegúrese de que todos los equipos protegidos puedan acceder a una carpeta de red compartida. Si la directiva de la organización no asegura el uso de una carpeta de red compartida en la red, se recomienda iniciar la tarea Generador de reglas para Control de dispositivos para las reglas de Control del equipo en el grupo de equipos de prueba o en una máquina modelo.

Agregar reglas generadas a la lista de reglas de Control de dispositivos

► *Para agregar las listas de reglas de autorización generadas a la tarea de Control de dispositivos:*

1. Abra la ventana **Reglas de Control de dispositivos** (consulte la sección "Cómo abrir la lista de reglas de Control de dispositivos" en la página 345).
2. Haga clic en el botón **Agregar**.
3. En el menú contextual del botón **Agregar**, seleccione la opción **Importar reglas desde archivo XML**.
4. Seleccione el principio para agregar las reglas de autorización generadas automáticamente a la lista de reglas de Control de dispositivos creadas anteriormente:
   - **Agregar a reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
   - **Reemplazar reglas existentes** si desea reemplazar las reglas existentes con las reglas importadas.
   - **Combinar con reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.
5. En la ventana estándar de Microsoft Windows que se abre, seleccione archivos XML creados después de la finalización de la tarea de grupo de Generador de reglas para Control de dispositivos.
6. Haga clic en **Abrir**.

   Todas las reglas generadas desde el archivo XML se agregan a la lista según el principio seleccionado.
7. Haga clic en el botón **Guardar** en la ventana **Reglas de Control de dispositivos**.
8. Si desea aplicar reglas generadas de Control de dispositivos, seleccione el modo de la tarea **Activar** en la configuración de la directiva **Control de dispositivos**.

Las reglas de autorización generadas automáticamente según datos del sistema en cada equipo independiente se aplican a todos los equipos de red abarcados por la directiva configurada. En estos equipos, la aplicación permitirá la conexión de solo los dispositivos para los cuales se crearon reglas de autorización.

Gestión del Control de dispositivos a través de la Consola de la aplicación

En esta sección, aprenda a navegar la interfaz de la Consola de la aplicación y establecer la configuración de la tarea en un equipo local.

En esta sección

Navegación

Sepa cómo navegar a la configuración de la tarea requerida a través de la interfaz.

En esta sección

Cómo abrir la configuración de la tarea de Control de dispositivos

► *Para abrir la configuración de la tarea de Control de dispositivos a través de la Consola de la aplicación:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Control de dispositivos**.
3. En el panel de detalles del nodo secundario **Control de dispositivos**, haga clic en el vínculo **Propiedades**.

   Se abre la ventana **Configuración de tareas**.
4. Configure la tarea como sea necesario.

Cómo abrir la ventana Reglas de control de dispositivos

► *Para abrir la lista de reglas de Control de dispositivos a través de la Consola de la aplicación:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Control de dispositivos**.
3. En el panel de detalles del nodo **Control de dispositivos**, haga clic en el vínculo **Reglas de Control de dispositivos**.

   Se abre la ventana **Reglas de Control de dispositivos**.
4. Configure la lista de reglas como sea necesario.

Cómo abrir la configuración de la tarea de Generador de reglas para Control de dispositivos

► *Para configurar la tarea Generador de reglas para Control de dispositivos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Generadores automatizados de reglas**.
2. Seleccione el nodo secundario **Generador de reglas para Control de dispositivos**.
3. En el panel de detalles del nodo secundario **Generador de reglas para Control de dispositivos**, haga clic en el vínculo **Propiedades**.

   Se abre la ventana **Configuración de tareas**.
4. Configure la tarea como sea necesario.

Configuración de la tarea Control de dispositivos

► *Para ajustar la configuración de la tarea Control de dispositivos:*

1. Abra la ventana **Configuración de tareas** (consulte la sección "Cómo abrir la configuración de la tarea de Control de dispositivos" en la página 355).
2. En la pestaña **General**, configure la siguiente configuración de tarea:
   - En la sección **Modo de la tarea**, seleccione uno de los modos de la tarea:
     - **Activar**.

       Kaspersky Embedded Systems Security aplica reglas para controlar la conexión de unidades flash y otros dispositivos externos, y autoriza o bloquea el uso de todos los dispositivos según el principio Denegar por defecto y las reglas de autorización especificadas. Se autoriza el uso de dispositivos externos de confianza. El uso de dispositivos externos dudosos sea bloquea de forma predeterminada.

       Si un dispositivo externo que se considera dudoso se conecta a un equipo protegido antes de que la tarea Control de dispositivos se ejecute en modo Activo, la aplicación no bloquea el dispositivo. Se recomienda desconectar el dispositivo dudoso manualmente o reiniciar el equipo. De lo contrario, el principio Denegar por defecto no se aplicará al dispositivo.

     - **Solo estadísticas**.

       Kaspersky Embedded Systems Security no controla la conexión de unidades flash ni otros dispositivos externos, sino que solo registra la información sobre la conexión y el registro de dispositivos externos en un equipo protegido y sobre las reglas de autorización de Control de dispositivos que activan los dispositivos conectados. Se autoriza el uso de todos los dispositivos externos. Este modo está configurado de forma predeterminada.
   - Seleccione o desactive la casilla de verificación **Permitir el uso de todos los dispositivos de almacenamiento masivo cuando la tarea Control de dispositivos no se esté ejecutando**.

     La casilla de verificación permite autorizar o bloquear el uso de dispositivos de almacenamiento masivo cuando la tarea de Control de dispositivos no se está ejecutando.

     Si la casilla está seleccionada y la tarea Control de dispositivos no se está ejecutando, Kaspersky Embedded Systems Security permite usar cualquier dispositivo de almacenamiento en un equipo protegido.

Si la casilla de verificación está desactivada, la aplicación bloquea el uso de dispositivos de almacenamiento masivo dudosos en un equipo protegido en los siguientes casos: la tarea de Control de dispositivos no se está ejecutando o el servicio de Kaspersky Security se ha detenido. Esta opción se recomienda para maximizar el nivel de protección contra las amenazas de seguridad informática que surgen al intercambiar archivos con dispositivos externos.

De forma predeterminada, la casilla está desactivada.

3. Si es necesario, en las pestañas **Programación** y **Avanzado**, configure las opciones de inicio de tareas programadas (consulte la sección “Configuración de las opciones de programación de inicio de tareas” en la página 149).
4. Para modificar la lista de reglas del control de dispositivos (consulte la sección "Acerca de las Reglas de Control de dispositivos" en la página 339), haga clic en el vínculo **Reglas de Control de dispositivos** en la parte inferior del panel de detalles del nodo **Control de dispositivos**.

Kaspersky Embedded Systems Security aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Configuración de las reglas de Control de dispositivos

Aprenda cómo generar, importar y exportar una lista de reglas o crear manualmente las reglas de autorización o denegación utilizando la tarea del Control de dispositivos.

En esta sección

Importación de reglas de Control de dispositivos desde un archivo XML

► *Para importar Reglas de Control de dispositivos, siga estos pasos:*

1. Abra la ventana **Reglas de Control de dispositivos** (consulte la sección "**Cómo abrir la ventana de reglas de Control de dispositivos**" en la página 355).
2. Haga clic en el botón **Agregar**.
3. En el menú contextual del botón, seleccione **Importar reglas desde archivo XML**.
4. Especifique el método para agregar reglas importadas. Para hacerlo, seleccione una de las opciones del menú contextual del botón **Importar reglas desde archivo XML**:
   - **Agregar a reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes.

Las reglas con configuración idéntica se duplican.

- **Reemplazar reglas existentes** si desea reemplazar las reglas existentes con las reglas importadas.
- **Combinar con reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

Se abre la ventana estándar **Abrir** de Microsoft Windows.

5. En la ventana **Abrir**, seleccione el archivo XML que contiene la configuración de las Reglas de Control de dispositivos.
6. Haga clic en el botón **Abrir**.

Las reglas importadas se mostrarán en la lista de la ventana **Reglas de Control de dispositivos**.

Llenado de la lista de reglas según los eventos de la tarea Control de dispositivos

► *Para crear un archivo de configuración que contenga listas de reglas de Control de dispositivos según los eventos de la tarea Control de dispositivos:*

1. Inicie la tarea de Control de dispositivos en el modo **Solo estadísticas** (consulte la sección "**Configuración de la tarea Control de dispositivos**" en la página 356) para registrar todos los eventos de conexiones a unidades flash y otros dispositivos externos a un equipo protegido.
2. Después de la finalización de la tarea en el modo **Solo estadísticas**, abra el registro de tareas con un clic en el botón **Abrir el registro de tareas** en la sección **Administración** del panel de detalles del nodo **Control de dispositivos**.
3. En la ventana **Registros**, haga clic en **Generar reglas basadas en los eventos**.

Kaspersky Embedded Systems Security creará un archivo XML de configuración que contendrá una lista de reglas generada según los eventos de la tarea de Control de dispositivos en el modo **Solo estadísticas**. Puede aplicar esta lista en la tarea Control de dispositivos (consulte la sección “Importación de las reglas de Control de dispositivos desde un archivo XML”, en la página 357).

Antes de aplicar una lista de reglas generada según los eventos de la tarea, se recomienda revisar y, luego, procesar manualmente la lista de reglas para asegurarse de que no haya dispositivos dudosos autorizados por las reglas especificadas.

Durante la conversión de un archivo XML con los eventos de la tarea a una lista de reglas, la aplicación genera reglas de autorización para todos los eventos registrados, incluidas las restricciones de dispositivos.

Todos los eventos de la tarea se registran en el registro de tareas sin tener en cuenta el modo de la tarea. Puede crear un archivo de configuración con una lista de reglas que se base en los eventos de la tarea en el modo **Activar**. Este método no se recomienda, excepto en casos urgentes en los que la eficacia de la tarea requiera la generación de una versión final de la lista de reglas antes de que la tarea se ejecute en el modo activo.

Cómo agregar una regla de autorización para uno o varios dispositivos externos

La tarea de Control de dispositivos no admite la función de adición manual de reglas de a una. Sin embargo, en casos donde debe agregar reglas para uno o varios dispositivos externos nuevos, puede usar la opción **Generar**

reglas basadas en datos del sistema. Si se aplica este escenario, la aplicación usa los datos de Windows sobre todos los dispositivos externos que se hayan conectado alguna vez y también autoriza a los dispositivos conectados en ese momento para el relleno de una lista de reglas de autorización.

Kaspersky Embedded Systems Security no obtiene el acceso a datos del sistema sobre los dispositivos móviles conectados mediante MTP. No puede generar reglas de autorización para dispositivos móviles conectados a MTP.

► *Para agregar una regla de autorización para uno o varios dispositivos externos que están conectados actualmente:*

1. Abra la ventana **Reglas de Control de dispositivos** (consulte la sección "Cómo abrir la ventana de reglas de Control de dispositivos" en la página 355).
2. Haga clic en el botón **Agregar**.
3. En el menú contextual que se abre, seleccione la opción **Generar reglas basadas en datos del sistema**.
4. En la ventana que se abre, revise la lista de dispositivos detectados y seleccione un solo dispositivo o varios en los que desee confiar en un equipo protegido.
5. Haga clic en el botón **Agregar reglas para los dispositivos seleccionados**.

Se generarán y se agregarán reglas nuevas a la lista de reglas de Control de dispositivos.

Eliminación de reglas de Control de dispositivos

► *Para eliminar las Reglas de Control de dispositivos:*

1. Abra la ventana **Reglas de Control de dispositivos** (consulte la sección "**Cómo abrir la ventana de reglas de Control de dispositivos**" en la página 355).
2. En la lista, seleccione una o varias reglas que desee eliminar.
3. Haga clic en el botón **Eliminar seleccionadas**.
4. Haga clic en el botón **Guardar**.

Las reglas de Control de dispositivos seleccionadas se eliminarán.

Exportación de reglas de Control de dispositivos

► *Para exportar Reglas del Control de dispositivos a un archivo de configuración:*

1. Abra la ventana **Reglas de Control de dispositivos** (consulte la sección "**Cómo abrir la ventana de reglas de Control de dispositivos**" en la página 355).
2. Haga clic el botón **Exportar a archivo**.

   Se abre la ventana de Microsoft Windows estándar.
3. En la ventana que se abre, especifique el archivo al cual desea exportar las reglas. Si no existe tal archivo, este se creará. Si ya existe un archivo con el nombre especificado, su contenido se volverá a escribir después de que las reglas se exporten.
4. Haga clic en el botón **Guardar**.

La regla y su configuración se exportarán al archivo especificado.

Habilitación y deshabilitación de reglas de Control de dispositivos

Puede habilitar y deshabilitar reglas de Control de dispositivos creadas sin eliminarlas.

► *Para habilitar y deshabilitar una regla de Control de dispositivos creada, siga estos pasos:*

1. Abra la ventana **Reglas de Control de dispositivos** (consulte la sección "**Cómo abrir la ventana de reglas de Control de dispositivos**" en la página 355).
2. En la lista de reglas especificadas, abra la ventana **Propiedades de la regla** con un clic doble en la regla cuyas propiedades desea configurar.
3. En la ventana que se abre, seleccione o desactive la casilla de verificación **Aplicar regla**.

   La casilla de verificación habilita o deshabilita una regla de Control de dispositivos.

   Si la casilla de verificación está seleccionada para una regla, la regla está activada. Se autoriza la conexión para dispositivos externos que se incluyen en el área de aplicación de las reglas.

   Si la casilla de verificación está desactivada en las propiedades de la regla, la regla está inactiva. Se bloquea la conexión para dispositivos externos que se incluyen en el área de aplicación de las reglas.

   De forma predeterminada, la casilla de verificación está seleccionada en la configuración de cada regla que se crea.
4. Haga clic en **Aceptar**.

El estado de aplicación de regla se guardará y se mostrará para la regla especificada.

Ampliación del área de aplicación de las reglas de Control de dispositivos

Cada regla de Control de dispositivos generada automáticamente abarca un solo dispositivo externo. Puede ampliar manualmente un área de aplicación de la regla si configura la máscara de la ruta de acceso a la instancia del dispositivo en las propiedades de cualquier regla especificada.

La aplicación de la ruta de acceso a la instancia del dispositivo reduce el número total de reglas especificadas y simplifica el procesamiento de las reglas. Sin embargo, la ampliación de un área de aplicación de la regla puede provocar la disminución de la eficacia del control de dispositivos de almacenamiento masivo.

► *Para aplicar una máscara a la ruta de acceso a la instancia del dispositivo en las propiedades de la regla de control de dispositivos:*

1. Abra la ventana **Reglas de Control de dispositivos** (consulte la sección "**Cómo abrir la ventana de reglas de Control de dispositivos**" en la página 355).
2. En la ventana que se abre, seleccione una regla para usar sus propiedades en la aplicación de la máscara.
3. Abra la ventana **Propiedades de la regla** con un doble clic en una regla de control de dispositivos seleccionada.
4. En la ventana que se abre, realice las siguientes operaciones:
   - Seleccione la casilla de verificación **Usar máscara** al lado del campo **Tipo de controlador (PID)** si desea que una regla seleccionada autorice conexiones para todos los dispositivos de almacenamiento masivo que coincidan con la información especificada sobre el fabricante del dispositivo y el número

de serie del dispositivo.

- Seleccione la casilla de verificación **Usar máscara** al lado del campo **Número de serie** si desea que una regla seleccionada autorice conexiones para todos los dispositivos de almacenamiento masivo que coincidan con la información especificada sobre el fabricante del dispositivo y el tipo de controlador.
- Seleccione las casillas de verificación **Usar máscara** al lado del campo **Tipo de controlador (PID)** y el campo **Número de serie** si desea que una regla seleccionada autorice conexiones para todos los dispositivos de almacenamiento masivo que coincidan con la información especificada sobre el fabricante del dispositivo.

Si la casilla **Usar máscara** está seleccionada en al menos uno de los campos, los datos de los campos con la casilla de verificación seleccionada son sustituidos por el signo * y no se tienen en cuenta cuando la regla se aplica.

5. Si es necesario, especifique información adicional sobre la regla en el campo **Descripción**. Por ejemplo, especifique los dispositivos afectados por la regla.
6. Haga clic en **Aceptar**.

Se guardarán las propiedades de la regla configuradas recientemente. El área de aplicación de la regla se ampliará según la máscara de la ruta de acceso a la instancia del dispositivo especificada.

Configuración de la tarea Generador de reglas para Control de dispositivos

► *Para configurar la tarea Generador de reglas para Control de dispositivos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Generadores automatizados de reglas**.
2. Seleccione el nodo secundario **Generador de reglas para Control de dispositivos**.
3. Haga clic en el vínculo **Propiedades** en el panel de detalles del nodo **Generador de reglas para Control de dispositivos**.

   Se abre la ventana **Configuración de tareas**.
4. En la pestaña **General**, seleccione modo de operación de la tarea en la sección **Modo de la tarea**:
   - **Tener en cuenta los datos del sistema sobre todas las unidades de almacenamiento masivo que se hayan conectado alguna vez**.
   - **Tener en cuenta solo las unidades de almacenamiento masivo conectadas actualmente**.
5. En la sección **Después de completada la tarea**, especifique las acciones que Kaspersky Embedded Systems Security debe realizar después de la finalización de la tarea:
   - **Agregar reglas de autorización a la lista de reglas de Control de dispositivos**.

     La casilla de verificación habilita o deshabilita la adición de reglas de autorización recientemente generadas a la lista de reglas de Control de dispositivos. La lista de reglas de Control de dispositivos se muestra cuando hace clic en el vínculo **Reglas de Control de dispositivos** en el panel de detalles del nodo **Control de dispositivos**.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security agrega las reglas generadas por la tarea de Generador de reglas para Control de dispositivos a la lista de reglas de Control de dispositivos, según el principio de adición seleccionado.

Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security no agrega las reglas de autorización recientemente generadas a la lista de reglas de Control de dispositivos. Las reglas generadas solo se exportan a un archivo.

De forma predeterminada, la casilla está activada.

La casilla de verificación no se puede seleccionar si la casilla de verificación **Exportar reglas de autorización a archivo** no está seleccionada.

- **Principio de adición**.

  La lista desplegable se utiliza para especificar el método utilizado para agregar las reglas de autorización recientemente generadas a la lista de reglas de Control de inicio de aplicaciones.

  - **Agregar a reglas existentes**. Las reglas se agregan a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
  - **Reemplazar reglas existentes**. Las reglas reemplazan a las reglas existentes en la lista.
  - **Combinar con reglas existentes**. Las reglas se agregan a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

  De forma predeterminada, está seleccionado el método **Combinar con reglas existentes**.

- **Exportar reglas de autorización a archivo**.

  La casilla de verificación habilita o deshabilita la exportación de reglas de autorización desde Control de dispositivos a un archivo.

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security exporta las reglas de autorización al archivo especificado en el campo a continuación cuando finaliza la tarea de Generador de reglas para Control de dispositivos.

  Si esta casilla se desactiva, la aplicación no exporta las reglas de autorización generadas a un archivo cuando finaliza la tarea del Generador de reglas para Control de dispositivos. En cambio, solo las agrega a la lista de reglas de Control de dispositivos.

  De forma predeterminada, la casilla está desactivada.

  La casilla de verificación no se puede seleccionar si la casilla de verificación **Agregar reglas de autorización a la lista de reglas de Control de dispositivos** no se seleccionó.

- **Agregar detalles del equipo al nombre del archivo**.

  La casilla de verificación habilita o deshabilita la adición de información sobre el equipo protegido al nombre del archivo al que se exportarán las reglas de autorización.

  Si esta casilla de verificación está seleccionada, la aplicación agrega el nombre del equipo protegido y la fecha y hora de creación del archivo al nombre del archivo de exportación.

  Si la casilla de verificación está desactivada, la aplicación no agrega información sobre el equipo protegido al nombre del archivo de exportación.

  De forma predeterminada, la casilla está activada.

6. En las pestañas **Programación** y **Avanzado**, configure las opciones de inicio de tareas programadas (consulte la sección “Configuración de las opciones de programación de inicio de tareas” en la página 149).
7. Haga clic en **Aceptar**.

Kaspersky Embedded Systems Security aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de auditoría del sistema.

Administración de firewall

Esta sección contiene información acerca de la tarea Administración de firewall y cómo configurarla.

En este capítulo

Acerca de la tarea Administración de firewall

Kaspersky Embedded Systems Security proporciona una solución confiable y ergonómica para proteger las conexiones de red mediante la tarea de administración del firewall.

La tarea de administración del firewall no realiza un filtrado de tráfico de red independiente, pero permite administrar el firewall de Windows por medio de la interfaz gráfica de Kaspersky Embedded Systems Security. Durante la tarea de administración del firewall, Kaspersky Embedded Systems Security controla la administración de la configuración y de las directivas del firewall del sistema operativo y bloquea cualquier posibilidad de configuración externa del firewall.

Durante la instalación de la aplicación, el componente de Administración de firewall lee y copia el estado del firewall de Windows y todas las reglas especificadas. Después de esto, solo es posible cambiar el conjunto de reglas y los parámetros de reglas, y activar o desactivar el firewall mediante Kaspersky Embedded Systems Security.

Si el firewall de Windows está desactivado durante la instalación de Kaspersky Embedded Systems Security, la tarea de administración del firewall no se ejecuta después de que finaliza la instalación. Si el firewall de Windows está activado durante la instalación de la aplicación, la tarea de Administración de firewall se ejecuta después de que la instalación finaliza. De esta manera, se bloquean todas las conexiones de red que las reglas especificadas no autorizan.

El componente de Administración de firewall no se instala de forma predeterminada, ya que no se incluye en el conjunto de componentes para la instalación recomendada.

La tarea de Administración de firewall aplica el bloqueo de todas las conexiones de entrada y de salida que no autorizan las reglas especificadas de la tarea.

La tarea sondea el firewall de Windows periódicamente y supervisa su estado. De forma predeterminada, el intervalo de sondeo está configurado en 1 minuto y no se puede cambiar. Si, durante el sondeo, Kaspersky Embedded Systems Security descubre diferencias entre la configuración del firewall de Windows y la configuración de la tarea de administración del firewall, la aplicación implementa la configuración de la tarea en el firewall del sistema operativo.

Con el sondeo del minuto por minuto del Firewall de Windows, Kaspersky Embedded Systems Security supervisa lo siguiente:

- Estado operativo del Firewall de Windows.
- Estado de reglas añadidas después de la instalación de Kaspersky Embedded Systems Security por otras aplicaciones o herramientas (por ejemplo, la adición de una nueva regla de aplicación para un puerto/aplicación mediante wf.msc).

Al aplicar las nuevas reglas al firewall de Windows, Kaspersky Embedded Systems Security crea un conjunto de reglas de Kaspersky Security Group en el complemento **Firewall de Windows**. Este conjunto de reglas une todas las reglas creadas por Kaspersky Embedded Systems Security usando la tarea de administración del firewall. Las reglas de grupo de Kaspersky Security no son supervisadas por la aplicación durante el sondeo cada minuto y no se sincronizan automáticamente con la lista de reglas especificadas en la configuración de la tarea de Administración de firewall.

► *Para actualizar las reglas de grupo de Kaspersky Security manualmente,*

reinicie la tarea de administración del firewall de Kaspersky Embedded Systems Security.

También puede corregir las reglas de Kaspersky Security Group manualmente mediante el complemento **Firewall de Windows**.

Si el firewall de Windows está controlado por la directiva de grupo de Kaspersky Security Center, la tarea de Administración de firewall no se puede iniciar.

Acerca de las reglas de firewall

La tarea de Administración de firewall controla el filtrado del tráfico de red de entrada y de salida mediante reglas de autorización que se aplican en el firewall de Windows durante la ejecución de la tarea.

La primera vez que la tarea se inicia, Kaspersky Embedded Systems Security lee y copia todas las reglas de tráfico de red de entrada especificadas en la configuración del firewall de Windows en la configuración de la tarea de administración del firewall. Luego, la aplicación funciona según las reglas siguientes:

- Si una nueva regla se crea en la configuración del firewall de Windows (de forma manual o automática durante una nueva instalación de aplicación), Kaspersky Embedded Systems Security elimina la regla.
- Si una regla existente se elimina de la configuración del firewall de Windows, Kaspersky Embedded Systems Security restaura la regla cuando se vuelva a iniciar tarea.
- Si los parámetros de una regla existente se cambian en la configuración del firewall de Windows, Kaspersky Embedded Systems Security revierte los cambios.
- Si una nueva regla se crea en la configuración de administración del firewall, Kaspersky Embedded Systems Security aplica la regla al firewall de Windows.
- Si una regla existente se elimina de la configuración de administración del firewall, Kaspersky Embedded Systems Security elimina la regla de la configuración del firewall de Windows.

Kaspersky Embedded Systems Security no trabaja con reglas de bloqueo ni reglas que controlen el tráfico de red saliente. Cuando se inicia la tarea de administración del firewall, Kaspersky Embedded Systems Security elimina todas reglas de ese tipo de la configuración del firewall de Windows.

Puede configurar, eliminar y editar las reglas de filtrado para el tráfico de red de entrada.

No puede especificar una nueva regla para controlar el tráfico de red saliente en la configuración de la tarea de Administración de firewall. Todas las reglas del firewall especificadas en Kaspersky Embedded Systems Security controlan solo el tráfico de red entrante.

Puede administrar los siguientes tipos de reglas de firewall:

- Reglas de aplicación.
- Reglas de puerto.

Reglas de aplicación

Este tipo de regla permite conexiones de red específicas para aplicaciones determinadas. El criterio de activación para estas reglas se basa en una ruta de acceso a un archivo ejecutable.

Puede administrar las reglas de aplicación:

- Agregar reglas nuevas.
- Eliminar reglas existentes.
- Habilitar y deshabilitar reglas específicas.
- Editar los parámetros de las reglas especificadas: especificar el nombre de la regla, la ruta de acceso del archivo ejecutable y el área de aplicación de la regla.

Reglas de puerto

Este tipo de regla permite las conexiones de red para los puertos y los protocolos especificados (TCP/UDP). Los criterios de activación para estas reglas se basan en el número de puerto y en el tipo de protocolo.

Puede administrar las reglas de puertos:

- Agregar reglas nuevas.
- Eliminar reglas existentes.
- Habilitar y deshabilitar reglas específicas.
- Editar los parámetros de las reglas especificadas: configurar el nombre de regla, el número de puerto, el tipo del protocolo y el área de aplicación de la regla.

Las reglas de puerto implican un área de aplicación más amplia que la de las reglas de aplicación. Al permitir conexiones basadas en reglas de puerto, baja el nivel de seguridad del equipo protegido.

Configuración predeterminada de la tarea de Administración de Firewall

La tarea de Administración de Firewall utiliza la configuración predeterminada que se describe en la tabla a continuación. Puede cambiar los valores de esta configuración.

Tabla 52. Configuración predeterminada de la tarea de Administración de Firewall

Configuración	Valor predeterminado	Descripción
Reglas de Firewall para la aplicación	Se habilitaron dos reglas predeterminadas para la aplicación	Puede deshabilitar las reglas predeterminadas o agregar nuevas reglas.
Reglas de Firewall para puertos	Se habilitaron seis reglas predeterminadas para puertos	Puede deshabilitar las reglas predeterminadas o agregar nuevas reglas.
Programación de inicio de tareas	La primera ejecución no está programada.	La tarea de Administración de Firewall no se inicia automáticamente al inicio de Kaspersky Embedded Systems Security. Puede configurar la programación de inicio de tareas.

Administración de las reglas del firewall mediante el Complemento de administración

En esta sección, aprenda cómo administrar las reglas del firewall mediante la interfaz de la Consola de la aplicación.

En esta sección

Habilitación y deshabilitación de Reglas de firewall

► *Para habilitar o deshabilitar una regla existente para filtrar el tráfico de red de entrada, realice las siguientes acciones:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.
4. En la sección **Control de actividad de red**, haga clic en el botón **Configurar** en la subsección **Administración de firewall**.
5. Haga clic en el botón **Lista de reglas** en la ventana que se abre.

   Se abre la ventana **Reglas de Firewall**.
6. Según el tipo de regla cuyo estado desee modificar, seleccione **Aplicaciones** o **Puertos**.
7. En la lista de reglas, seleccione la regla cuyo estado desee modificar y realice una de las acciones siguientes:
   - Si desea habilitar una regla deshabilitada, seleccione la casilla de verificación ubicada a la izquierda del nombre de la regla.

     La regla seleccionada se habilitará.
   - Si desea deshabilitar una regla habilitada, desactive la casilla de verificación ubicada a la izquierda del nombre de la regla.

     La regla seleccionada se deshabilitará.
8. Haga clic en **Aceptar** en la ventana **Reglas de firewall**.
9. Haga clic en **Aceptar** en la ventana **Administración de firewall**.
10. Haga clic en **Aceptar** en la ventana **Propiedades: <Nombre de la directiva>**.

Se guarda la configuración de la tarea especificada. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Cómo agregar manualmente reglas de firewall

Solo puede agregar y editar reglas para aplicaciones y para puertos. No puede agregar reglas de grupo nuevas ni editar las existentes.

► *Para agregar una regla nueva o editar una existente para filtrar el tráfico de red de entrada, realice lo siguiente:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.
4. En la sección **Control de actividad de red**, haga clic en el botón **Configurar** en la subsección **Administración de firewall**.
5. Haga clic en el botón **Lista de reglas** en la ventana que se abre.

   Se abre la ventana **Reglas de Firewall**.
6. Según el tipo de regla que desee agregar, seleccione la pestaña **Aplicaciones** o **Puertos** y realice una de las acciones siguientes:
   - Para editar una regla existente, seleccione la regla que desee editar en la lista de reglas y haga clic en **Editar**.
   - Para agregar una nueva regla, haga clic en **Agregar**.

     Según el tipo de regla que se vaya a configurar, se abre la ventana **Regla de puerto** o la de **Regla de aplicación**.
7. En la ventana que se abre, realice las siguientes operaciones:
   - Si está trabajando con una regla de aplicación, realice lo siguiente:
     a. Ingrese el **Nombre de regla** de la regla editada.
     b. Especifique la **Ruta de aplicación** del archivo ejecutable de la aplicación para la cual se está autorizando una conexión mediante la modificación de esta regla.

        Puede configurar la ruta de acceso manualmente o mediante el botón **Examinar**.
     c. En el campo **Área de aplicación de regla**, especifique las direcciones de red para las cuales se

aplicará la regla modificada.

> Solo puede usar direcciones IP de tipo IPv4.

- Si está trabajando con una regla de puerto, realice lo siguiente:
  a. Ingrese el **Nombre de regla** de la regla editada.
  b. Especifique el **Número de puerto** para el cual la aplicación autorizará las conexiones.
  c. Seleccione el tipo de protocolo (TCP/UDP) para el cual la aplicación autorizará las conexiones.
  d. En el campo **Área de aplicación de regla**, especifique las direcciones de red para las cuales se aplicará la regla modificada.

> Solo puede usar direcciones IP de tipo IPv4.

8. Haga clic en **Aceptar** en la ventana **Regla de Aplicación** o **Regla de puerto**.
9. Haga clic en **Aceptar** en la ventana **Administración de firewall**.
10. Haga clic en **Aceptar** en la ventana **Propiedades: <Nombre de la directiva>**.

Se guarda la configuración de la tarea especificada. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Eliminación de reglas de firewall

> Solo puede eliminar reglas de puerto y de aplicación. No puede eliminar reglas de grupo existentes.

► *Para eliminar una regla existente para filtrar el tráfico de red de entrada, realice las siguientes acciones:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

> Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.

4. En la sección **Control de actividad de red**, haga clic en el botón **Configurar** en la subsección **Administración de firewall.**
5. Haga clic en el botón **Lista de reglas** en la ventana que se abre.

   Se abre la ventana **Reglas de Firewall**.
6. Según el tipo de regla cuyo estado desee modificar, seleccione la pestaña **Aplicaciones** o **Puertos**.
7. En la lista de reglas, seleccione la regla que desee eliminar.
8. Haga clic en el botón **Eliminar**.

   La regla seleccionada se elimina.
9. Haga clic en **Aceptar** en la ventana **Reglas de firewall**.
10. Haga clic en **Aceptar** en la ventana **Administración de firewall**.
11. Haga clic en **Aceptar** en la ventana **Propiedades: <Nombre de la directiva>**.

Se guardará la configuración especificada para la tarea de Administración de firewall. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Administración de las reglas del firewall mediante la Consola de la aplicación

En esta sección, aprenda cómo administrar las reglas del firewall mediante la interfaz de la Consola de la aplicación.

En esta sección

Habilitación y deshabilitación de Reglas de firewall

► *Para habilitar o deshabilitar una regla existente para filtrar el tráfico de red de entrada, realice las siguientes acciones:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Administración de firewall**.
3. Haga clic en el vínculo **Reglas de Firewall** en el panel de detalles del nodo **Administración de firewall**.

   Se abre la ventana **Reglas de Firewall**.
4. Según el tipo de regla cuyo estado desee modificar, seleccione **Aplicaciones** o **Puertos**.
5. En la lista de reglas, seleccione la regla cuyo estado desee modificar y realice una de las acciones siguientes:
   - Si desea habilitar una regla deshabilitada, seleccione la casilla de verificación ubicada a la izquierda

del nombre de la regla.

La regla seleccionada se habilitará.

- Si desea deshabilitar una regla habilitada, desactive la casilla de verificación ubicada a la izquierda del nombre de la regla.

  La regla seleccionada se deshabilitará.

6. Haga clic en **Guardar** en la ventana **Reglas de firewall**.

Se guarda la configuración de la tarea especificada. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Cómo agregar manualmente reglas de firewall

► *Para agregar una regla nueva o editar una existente para filtrar el tráfico de red de entrada, realice lo siguiente:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Administración de firewall**.
3. Haga clic en el vínculo **Reglas de Firewall** en el panel de detalles del nodo **Administración de firewall**.

   Se abre la ventana **Reglas de Firewall**.
4. Según el tipo de regla que desee agregar, seleccione la pestaña **Aplicaciones** o **Puertos** y realice una de las acciones siguientes:
   - Para editar una regla existente, seleccione la regla que desee editar en la lista de reglas y haga clic en **Editar**.
   - Para agregar una nueva regla, haga clic en **Agregar**.

     Según el tipo de regla que se vaya a configurar, se abre la ventana **Regla de puerto** o la de **Regla de aplicación**.
5. En la ventana que se abre, realice las siguientes operaciones:
   - Si está trabajando con una regla de aplicación, realice lo siguiente:
     a. Ingrese el **Nombre de regla** de la regla editada.
     b. Especifique la **Ruta de aplicación** del archivo ejecutable de la aplicación para la cual se está autorizando una conexión mediante la modificación de esta regla.

        Puede configurar la ruta de acceso manualmente o mediante el botón **Examinar**.
     c. En el campo **Área de aplicación de regla**, especifique las direcciones de red para las cuales se aplicará la regla modificada.

     > Solo puede usar direcciones IP de tipo IPv4.

   - Si está trabajando con una regla de puerto, realice lo siguiente:
     a. Ingrese el **Nombre de regla** de la regla editada.
     b. Especifique el **Número de puerto** para el cual la aplicación autorizará las conexiones.
     c. Seleccione el tipo de protocolo (TCP/UDP) para el cual la aplicación autorizará las conexiones.
     d. En el campo **Área de aplicación de regla**, especifique las direcciones de red para las cuales se

aplicará la regla modificada.

> Solo puede usar direcciones IP de tipo IPv4.

6. Haga clic en **Aceptar** en la ventana **Regla de Aplicación** o **Regla de puerto**.
7. Haga clic en **Guardar** en la ventana **Reglas de firewall**.

Se guarda la configuración de la tarea especificada. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Eliminación de reglas de firewall

> Solo puede eliminar reglas de puerto y de aplicación. No puede eliminar reglas de grupo existentes.

► *Para eliminar una regla existente para filtrar el tráfico de red de entrada, realice las siguientes acciones:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Control del equipo**.
2. Seleccione el nodo secundario **Administración de firewall**.
3. Haga clic en el vínculo **Reglas de Firewall** en el panel de detalles del nodo **Administración de firewall**.

   Se abre la ventana **Reglas de Firewall**.
4. Según el tipo de regla cuyo estado desee modificar, seleccione la pestaña **Aplicaciones** o **Puertos**.
5. En la lista de reglas, seleccione la regla que desee eliminar.
6. Haga clic en el botón **Eliminar**.

   La regla seleccionada se elimina.
7. Haga clic en **Guardar** en la ventana **Reglas de firewall**.

Se guarda la configuración de la tarea especificada. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Monitor de integridad de archivos

Esta sección contiene información sobre el inicio y la configuración de la tarea Monitor de integridad de archivos.

En este capítulo

Acerca de la tarea del Monitor de integridad de archivos

La tarea Monitor de integridad de archivos se diseña para realizar un seguimiento de las acciones realizadas con los archivos y las carpetas especificados en las áreas de aplicación especificadas en la configuración de la tarea. Puede usar la tarea de detectar los cambios en el archivo que podrían indicar una violación de la seguridad en el equipo protegido. También puede configurar que se realice un seguimiento de los cambios en el archivo durante periodos en los cuales la supervisión se interrumpe.

Una *interrupción de supervisión* ocurre cuando el área de supervisión temporalmente queda fuera del área de la tarea, por ejemplo, si la tarea se detiene o si un dispositivo de almacenamiento masivo no está físicamente presente en un equipo protegido. Kaspersky Embedded Systems Security informa las operaciones con archivos detectadas en el área de supervisión tan pronto como un dispositivo de almacenamiento se conecta de nuevo.

Si las tareas dejan de ejecutarse en el área de supervisión especificada debido a una nueva instalación del componente Monitor de integridad de archivos, esto no constituye una interrupción de supervisión. En este caso, la tarea del Monitor de integridad de archivos no se ejecuta.

Requisitos en el entorno

Para iniciar la tarea del Monitor de integridad de archivos, se deben cumplir las siguientes condiciones:

- Un dispositivo de almacenamiento masivo que admite ReFS y sistemas de archivos NTFS se deben instalar en el equipo protegido.
- Se debe habilitar el diario de USN de Windows. El componente le solicita a este diario recibir la información sobre operaciones con archivos.

  Si habilita el diario de USN después de que una regla se haya creado para un volumen y la tarea del Monitor de integridad de archivos se ha iniciado, la tarea se debe reiniciar. Si no, la regla no se aplicará durante la supervisión.

Áreas de supervisión excluidas

Puede crear áreas de supervisión excluidas (consulte la sección "Configuración de las reglas de supervisión" en la página 379). Las exclusiones se especifican para cada regla independiente y funcionan solo para el área de supervisión indicada. Puede especificar un número ilimitado de exclusiones para cada regla.

> Las exclusiones tienen mayor prioridad que el área de supervisión y no son supervisadas por la tarea, aun si una carpeta o el archivo indicado están dentro del área de supervisión. Si la configuración para una de las reglas especifica un área de supervisión a un nivel inferior que una carpeta especificada en exclusiones, el área de supervisión no se considera cuando la tarea se ejecuta.

Para especificar exclusiones, puede usar las mismas máscaras que se usan para especificar áreas de supervisión.

Acerca de las reglas de supervisión de las operaciones con archivos

El Monitor de integridad de archivos se ejecuta según reglas de supervisión de operación con archivos. Puede usar los criterios de activación de la regla para configurar las condiciones que desencadenan la tarea y ajustan el nivel de importancia de eventos para operaciones con archivos detectadas y registradas en el registro de tareas.

Una regla de supervisión de operación con archivos se especifica para cada área de supervisión.

Puede configurar los siguientes criterios de activación de la regla:

- Usuarios de confianza.
- Marcadores de operaciones con archivos.

Usuarios de confianza

De forma predeterminada, la aplicación trata todas las acciones del usuario como posible violación de la seguridad. La lista de usuarios de confianza está vacía. Puede configurar el nivel de importancia del evento al crear una lista de usuarios de confianza en la operación con archivos que supervisa la configuración de la regla.

Usuario que no es de confianza: cualquier usuario no indicado en la lista de usuarios de confianza en la configuración de la regla del área de supervisión. Si Kaspersky Embedded Systems Security detecta una operación con archivos realizada por un usuario que no es de confianza, la tarea del Monitor de integridad de archivos registra un Evento crítico en el registro de tareas.

Usuario de confianza: un usuario o el grupo de usuarios autorizados para realizar operaciones con archivos en el área de supervisión especificada. Si Kaspersky Embedded Systems Security detecta operaciones con archivos realizadas por un usuario de confianza, la tarea del Monitor de integridad de archivos registra un Evento informativo en el registro de tareas.

Kaspersky Embedded Systems Security no puede determinar a los usuarios que inician operaciones durante los períodos de interrupción de la supervisión. En este caso, el estado del usuario está determinado como desconocido.

Usuario desconocido: este estado se asigna a un usuario si Kaspersky Embedded Systems Security no puede recibir la información sobre un usuario debido a una interrupción de la tarea o una omisión del controlador de sincronización de datos o un diario de USN. Si Kaspersky Embedded Systems Security detecta una operación con archivos realizada por un usuario desconocido, la tarea del Monitor de integridad de archivos registra un evento de *Advertencia* en el registro de tareas.

Marcadores de operaciones con archivos

Cuando la tarea del Monitor de integridad de archivos se ejecuta, Kaspersky Embedded Systems Security usa marcadores de operaciones con archivos para decidir que una acción se ha realizado en un archivo.

Un marcador de operaciones con archivos es un descriptor único que puede caracterizar una operación con archivos.

Cada operación con archivos puede ser una sola acción o una cadena de acciones con archivos. Cada acción de esta clase se compara con un marcador de operaciones con archivos. Si el marcador que especifica como criterio de activación de la regla se detecta en una cadena de operaciones con archivos, la aplicación registra un evento que indica que la operación con archivos dada se realizó.

El nivel de importancia de los eventos registrados no depende de los marcadores de operaciones con archivos seleccionados o el número de eventos.

De forma predeterminada, Kaspersky Embedded Systems Security considera todos los marcadores de operaciones con archivos disponibles. Puede seleccionar marcadores de operaciones con archivos manualmente en la configuración de la regla de la tarea.

Tabla 53. Marcadores de operaciones con archivos

ID de operación con archivos	Marcador de operaciones con archivos	Sistemas de archivos admitidos
BASIC_INFO_CHANGE	Los atributos o los marcadores del tiempo de un archivo o carpeta cambiaron.	NTFS, ReFS
COMPRESSION_CHANGE	La compresión de un archivo o carpeta cambió.	NTFS, ReFS
DATA_EXTEND	El tamaño de archivo o carpeta aumentó.	NTFS, ReFS
DATA_OVERWRITE	El dato en un archivo o carpeta se sobrescribió.	NTFS, ReFS
DATA_TRUNCATION	Archivo o carpeta truncados.	NTFS, ReFS
EA_CHANGE	Los atributos de la carpeta o el archivo ampliado cambiaron.	Solo NTFS
ENCRYPTION_CHANGE	El estado del cifrado del archivo o la carpeta cambió.	NTFS, ReFS
FILE_CREATE	Archivo o carpeta creada por primera vez	NTFS, ReFS
FILE_DELETE	El archivo o la carpeta eliminados de forma permanente con la combinación SHIFT+DEL	NTFS, ReFS
HARD_LINK_CHANGE	Vínculo físico creado o eliminado del archivo o la carpeta	Solo NTFS
INDEXABLE_CHANGE	El estado del índice de archivo o carpeta cambió.	NTFS, ReFS
INTEGRITY_CHANGE	El atributo de integridad cambió para un determinado flujo de archivos.	Solo ReFS
NAMED_DATA_EXTEND	El tamaño de un determinado flujo de archivos aumentó.	NTFS, ReFS
NAMED_DATA_OVERWRITE	Determinado flujo de archivos sobrescrito	NTFS, ReFS

ID de operación con archivos	Marcador de operaciones con archivos	Sistemas de archivos admitidos
NAMED_DATA_TRUNCATION	Determinado flujo de archivos truncado	NTFS, ReFS
OBJECT_ID_CHANGE	El identificador de archivo o carpeta cambió.	NTFS, ReFS
RENAME_NEW_NAME	Nombre nuevo asignado a archivo o carpeta	NTFS, ReFS
REPARSE_POINT_CHANGE	Nuevo punto de reanálisis creado o existente cambiado para un archivo o carpeta	NTFS, ReFS
SECURITY_CHANGE	Los derechos de acceso del archivo o la carpeta cambiaron.	NTFS, ReFS
STREAM_CHANGE	Determinado flujo de archivos nuevo creado o flujo de archivos existentes modificado	NTFS, ReFS
TRANSACTED_CHANGE	Flujo de archivos determinado modificado por transacción TxF	Solo ReFS

Configuración de la tarea del Monitor de integridad de archivos predeterminada

De forma predeterminada, la tarea del Monitor de integridad de archivos tiene la configuración descrita en la tabla a continuación. Puede cambiar los valores de esta configuración.

Tabla 54. Configuración de la tarea del Monitor de integridad de archivos predeterminada

Configuración	Valor predeterminado	Descripción
Área de supervisión	No configurado	Puede especificar las carpetas y los archivos para los cuales las acciones se supervisarán. Los eventos de supervisión se generarán para las carpetas y los archivos en el área de supervisión especificada.
Lista de usuarios de confianza	No configurado	Puede especificar a usuarios o grupos de usuarios cuyas acciones en las carpetas especificadas serán tratadas como seguras por el componente.
Supervise operaciones con archivos cuando la tarea no se ejecute	Utilizado	Puede habilitar o deshabilitar el registro de operaciones con archivos realizadas en el área de supervisión indicado durante los periodos en los que no se ejecuta la tarea.
Excluir las siguientes carpetas del control	No aplicado	Puede examinar el uso de exclusiones para ver carpetas donde las operaciones con archivos no se tienen que supervisar. Cuando la tarea Monitor de integridad de archivos se ejecute, Kaspersky Embedded Systems Security omitirá las áreas de supervisión especificada como exclusiones.

Configuración	Valor predeterminado	Descripción
Cálculo de la suma de control	No aplicado	Puede configurar el cálculo de la suma de control del archivo después de aplicar los cambios en el archivo.
Considerar los marcadores de operaciones con archivos	Todos los marcadores de operaciones con archivos disponibles se consideran.	Puede especificar el conjunto de marcadores de operaciones con archivos. Si una operación con archivos realizada en un área de supervisión es caracterizada por uno o varios marcadores especificados, Kaspersky Embedded Systems Security genera un evento de auditoría.
Programación de inicio de tareas	La primera ejecución no está programada	Puede configurar las opciones del inicio programado de la tarea.

Administración de Monitor de integridad de archivos mediante el Complemento de administración

En esta sección, aprenda cómo configurar la tarea de Monitor de integridad de archivos mediante el Complemento de administración.

En esta sección

Configuración de las opciones de la tarea del Monitor de integridad de archivos

Para configurar los parámetros generales del Monitor de integridad de archivos, siga estos pasos:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.

4. En la sección **Inspección del sistema** en el bloque **Monitor de integridad de archivos**, haga clic en el botón **Configurar**.

   Se abre la ventana **Monitor de integridad de archivos**.

5. En la pestaña **Configuración de supervisión de operaciones de archivos** en la ventana que se abre, ajuste la configuración del área de supervisión:

   a. Seleccionar o desactivar la casilla de verificación **Registrar la información sobre las operaciones de los archivos que aparece durante el período de interrupción de la supervisión**.

      La casilla habilita o deshabilita la supervisión de las operaciones con archivos especificadas en la configuración de la tarea del Monitor de integridad de archivos cuando la tarea no se está ejecutando por ningún motivo (la eliminación de un disco duro, la tarea fue detenida por usuario, error de software).

      Si la casilla se selecciona, Kaspersky Embedded Systems Security registrará eventos en todas las áreas de supervisión cuando la tarea del Monitor de integridad de archivos no se ejecute.

      Si la casilla se desactiva, la aplicación no registrará las operaciones con archivos en las áreas de supervisión cuando la tarea no se esté ejecutando.

      De forma predeterminada, la casilla está activada.

   b. Agregue las áreas de supervisión (consulte la sección “Configuración de reglas de supervisión”, en la página 379) que la tarea debe supervisar.

6. En la ficha **Administración de la tarea**, configure los parámetros de inicio de tareas en base a una programación (consulte la sección “Administración de programaciones de tareas”, en la página 128).

7. Haga clic en **Aceptar** para guardar los cambios.

Configuración de reglas de supervisión

Puede cambiar las configuraciones predeterminadas de la tarea del Monitor de Integridad de archivos (ver la siguiente tabla).

Tabla 55. Configuración de la tarea del Monitor de integridad de archivos predeterminada

Configuración	Valor predeterminado	Descripción
Área de supervisión	No configurado	Puede especificar las carpetas y los archivos para los cuales las acciones se supervisarán. Los eventos de supervisión se generarán para las carpetas y los archivos en el área de supervisión especificada.
Lista de usuarios de confianza	No configurado	Puede especificar a usuarios o grupos de usuarios cuyas acciones en las carpetas especificadas serán tratadas como seguras por el componente.
Supervise operaciones con archivos cuando la tarea no se ejecute	Utilizado	Puede habilitar o deshabilitar el registro de operaciones con archivos realizadas en el área de supervisión indicado durante los periodos en los que no se ejecuta la tarea.

Configuración	Valor predeterminado	Descripción
Excluir las siguientes carpetas del control	No aplicado	Puede examinar el uso de exclusiones para ver carpetas donde las operaciones con archivos no se tienen que supervisar. Cuando la tarea Monitor de integridad de archivos se ejecute, Kaspersky Embedded Systems Security omitirá las áreas de supervisión especificada como exclusiones.
Cálculo de la suma de control	No aplicado	Puede configurar el cálculo de la suma de control del archivo después de aplicar los cambios en el archivo.
Considerar los marcadores de operaciones con archivos	Todos los marcadores de operaciones con archivos disponibles se consideran.	Puede especificar el conjunto de marcadores de operaciones con archivos. Si una operación con archivos realizada en un área de supervisión es caracterizada por uno o varios marcadores especificados, Kaspersky Embedded Systems Security genera un evento de auditoría.
Programación de inicio de tareas	La primera ejecución no está programada	Puede configurar las opciones del inicio programado de la tarea.

► *Para agregar un área de supervisión, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

     Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.
4. En la sección **Inspección del sistema** en el bloque **Monitor de integridad de archivos**, haga clic en el botón **Configurar**.

   Se abre la ventana **Propiedades:** Se abre la ventana **Monitor de integridad de archivos**.
5. En la sección **Área de supervisión**, haga clic en el botón **Agregar**.

   Se abre la ventana **Área de supervisión**.

6. Agregue un área de supervisión de una de las siguientes maneras:
   - Si desea seleccionar carpetas a través del diálogo estándar de Microsoft Windows:
     a. Haga clic en el botón **Examinar**.

        Se abre la ventana estándar Buscar carpeta de Microsoft Windows.

     b. En la ventana que se abre, seleccione la carpeta para la cual desea supervisar operaciones y haga clic en el botón **Aceptar**.
   - Si desea especificar un área de supervisión manualmente, agregue una ruta mediante una máscara admitida:
     - <*.ext>: todos los archivos con la extensión <ext>, sin tener en cuenta su ubicación;
     - <*\name.ext>: todos los archivos con nombre <nombre> y extensión <ext>, sin tener en cuenta su ubicación;
     - <\dir*> - todos los archivos en la carpeta <\dir>;
     - <\dir*\name.ext>: todos los archivos con el nombre <nombre> y la extensión <ext> en la carpeta <\dir> y todas sus carpetas secundarias.

   Al especificar un área de supervisión manualmente, asegúrese de que la ruta esté en el formato siguiente: <letra del volumen>: \<máscara>. Si la letra del volumen falta, Kaspersky Embedded Systems Security no agregará el área de supervisión especificada.

7. En la pestaña **Usuarios de confianza**, haga clic en el botón **Agregar**.

   Se abre la ventana estándar **Seleccionar usuarios o grupos** de Microsoft Windows.

8. Seleccione los usuarios o los grupos de usuarios para los que están autorizadas las operaciones con archivos en el área de supervisión seleccionada y haga clic en el botón **Aceptar**.

   De forma predeterminada, Kaspersky Embedded Systems Security trata a todos los usuarios que no figuran en la lista de usuarios de confianza como dudosos (consulte la sección “Acerca de las reglas de supervisión de las operaciones con archivos” en la página 375), y genera eventos críticos para ellos.

9. Seleccione la pestaña **Marcadores de operación de los archivos**.
10. Si es necesario, realice las siguientes acciones para seleccionar varios marcadores:
    a. Seleccione la opción **Detectar las operaciones de archivos sobre la base de los siguientes marcadores**.
    b. En la lista de operaciones con archivos disponibles (consulte la sección “Acerca de las reglas de supervisión de operaciones con archivos”, en la página 375), seleccione las casillas de verificación ubicadas junto a las operaciones que desea supervisar.

    De manera predeterminada, Kaspersky Embedded Systems Security detecta todos los marcadores de operaciones con archivos, ya que está seleccionada la opción **Detectar las operaciones de archivos sobre la base de todos los marcadores reconocibles**.

11. Si desea que Kaspersky Embedded Systems Security calcule la suma de control de archivos después de que la operación se realiza, haga lo siguiente:

    a. Seleccione la opción **Calcular la suma de control para el archivo de ser posible.** La casilla de verificación de **La suma de control podrá visualizarse en el informe de la tarea**.

       Si la casilla se selecciona, Kaspersky Embedded Systems Security calcula la suma de control del archivo modificado, donde se detectó la operación con archivos con al menos un marcador.

       Si la operación con archivos es detectada por varios marcadores, solo se calcula la suma de control del archivo final después de que todas las modificaciones.

       Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no calcula la suma de control para los archivos modificados.

       Ningún cálculo de la suma de control se realiza en los casos siguientes:

       - Si el archivo se volviera no disponible (por ejemplo, debido al cambio de permisos de acceso).
       - Si la operación con archivos se detecta en el archivo que se ha eliminado después.

       De forma predeterminada, la casilla está desactivada.

    b. En la lista desplegable **Calcular la suma de control que usa el algoritmo**, seleccione una de las opciones:

       - **Hash MD5**
       - **Hash SHA256**

12. Si no desea supervisar todas las operaciones con archivos en la lista de operaciones con archivos disponibles (consulte la sección “Acerca de las reglas de supervisión de operación de archivos”, en la página 375) y seleccione las casillas de verificación ubicadas junto a las operaciones que desea supervisar.
13. Si es necesario, agregue áreas de supervisión excluidas al realizar los pasos siguientes:

    a. Seleccione la pestaña **Exclusiones**.

    b. Seleccione la casilla de verificación **Excluir las siguientes carpetas del control**.

       La casilla deshabilita el uso de exclusiones para carpetas donde las operaciones con archivos no se tienen que supervisar.

       Si la casilla se selecciona, Kaspersky Embedded Systems Security omite las áreas de alcance especificadas en la lista de exclusiones cuando la tarea del Monitor de integridad de archivos se ejecuta.

       Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security registra los eventos de todas las áreas de supervisión especificadas.

       De forma predeterminada, la casilla se desactiva y la lista de exclusión aparece vacía.

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

       La ventana **Seleccionar carpeta para agregar** se abre.

    d. En la ventana que se abre, especifique el objeto que desea excluir del área de supervisión.

    e. Haga clic en **Aceptar**.

       La carpeta especificada se añade a la lista de áreas excluidas.

14. Haga clic en **Aceptar** en la ventana **Regla de supervisión de operaciones de archivos**.

    La configuración de la regla especificada se aplicará al área de supervisión seleccionada de la tarea del Monitor de integridad de archivos.

Administración de Monitor de integridad de archivos mediante la Consola de la aplicación

En esta sección, aprenda cómo configurar la tarea de Monitor de integridad de archivos mediante la Consola de la aplicación.

En esta sección

Configuración de las opciones de la tarea del Monitor de integridad de archivos

► *Para configurar los parámetros generales del Monitor de integridad de archivos, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Inspección del sistema**.
2. Seleccione el nodo secundario **Monitor de integridad de archivos**.
3. Haga clic en el vínculo **Propiedades** en el panel de detalles del nodo **Monitor de integridad de archivos**.

   Se abre la ventana **Configuración de tareas**.
4. En la ventana que se abre, en la pestaña **General**, desactive o seleccione la casilla de verificación **Registrar información de las operaciones del archivo que aparecen durante el período de interrupción del control**.

   La casilla habilita o deshabilita la supervisión de las operaciones con archivos especificadas en la configuración de la tarea del Monitor de integridad de archivos cuando la tarea no se está ejecutando por ningún motivo (la eliminación de un disco duro, la tarea fue detenida por usuario, error de software).

   Si la casilla se selecciona, Kaspersky Embedded Systems Security registrará eventos en todas las áreas de supervisión cuando la tarea del Monitor de integridad de archivos no se ejecute.

   Si la casilla se desactiva, la aplicación no registrará las operaciones con archivos en las áreas de supervisión cuando la tarea no se esté ejecutando.

   De forma predeterminada, la casilla está activada.
5. En las pestañas **Programación** y **Avanzado**, configure la programación de inicio de tareas (consulte la sección “Administración de programaciones de tareas” en la página 128).
6. Haga clic en **Aceptar** para guardar los cambios.

Configuración de reglas de supervisión

Puede cambiar las configuraciones predeterminadas de la tarea del Monitor de Integridad de archivos (ver la siguiente tabla).

Tabla 56. Configuración de la tarea del Monitor de integridad de archivos predeterminada

Configuración	Valor predeterminado	Descripción
Área de supervisión	No configurado	Puede especificar las carpetas y los archivos para los cuales las acciones se supervisarán. Los eventos de supervisión se generarán para las carpetas y los archivos en el área de supervisión especificada.
Lista de usuarios de confianza	No configurado	Puede especificar a usuarios o grupos de usuarios cuyas acciones en las carpetas especificadas serán tratadas como seguras por el componente.
Supervise operaciones con archivos cuando la tarea no se ejecute	Utilizado	Puede habilitar o deshabilitar el registro de operaciones con archivos realizadas en el área de supervisión indicado durante los periodos en los que no se ejecuta la tarea.
Excluir las siguientes carpetas del control	No aplicado	Puede examinar el uso de exclusiones para ver carpetas donde las operaciones con archivos no se tienen que supervisar. Cuando la tarea Monitor de integridad de archivos se ejecute, Kaspersky Embedded Systems Security omitirá las áreas de supervisión especificada como exclusiones.
Cálculo de la suma de control	No aplicado	Puede configurar el cálculo de la suma de control del archivo después de aplicar los cambios en el archivo.
Considerar los marcadores de operaciones con archivos	Todos los marcadores de operaciones con archivos disponibles se consideran.	Puede especificar el conjunto de marcadores de operaciones con archivos. Si una operación con archivos realizada en un área de supervisión es caracterizada por uno o varios marcadores especificados, Kaspersky Embedded Systems Security genera un evento de auditoría.
Programación de inicio de tareas	La primera ejecución no está programada	Puede configurar las opciones del inicio programado de la tarea.

► *Para agregar un área de supervisión, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Inspección del sistema**.
2. Seleccione el nodo secundario **Monitor de integridad de archivos**.
3. Haga clic en el vínculo **Regla de Monitor de integridad de archivos** en el panel de detalles del nodo **Monitor de integridad de archivos**.

   Se abre la ventana **Supervisión de operaciones de archivo**.

4. Agregue un área de supervisión de una de las siguientes maneras:
   - Si desea seleccionar carpetas a través del diálogo estándar de Microsoft Windows:
     a. En el lado izquierdo de la ventana, haga clic en el botón **Examinar**.

        Se abre la ventana estándar **Buscar carpeta** de Microsoft Windows.

     b. En la ventana que se abre, seleccione la carpeta para la cual desea supervisar operaciones y haga clic en el botón **Aceptar**.

     c. Haga clic el botón **Agregar** para que Kaspersky Embedded Systems Security comience a supervisar operaciones con archivos en el área de supervisión indicada.
   - Si desea especificar un área de supervisión manualmente, agregue una ruta mediante una máscara admitida:
     - <*.ext>: todos los archivos con la extensión <ext>, sin tener en cuenta su ubicación;
     - <*\name.ext>: todos los archivos con nombre <nombre> y extensión <ext>, sin tener en cuenta su ubicación;
     - <\dir*> - todos los archivos en la carpeta <\dir>;
     - <\dir*\name.ext>: todos los archivos con el nombre <nombre> y la extensión <ext> en la carpeta <\dir> y todas sus carpetas secundarias.

   > Al especificar un área de supervisión manualmente, asegúrese de que la ruta esté en el formato siguiente: <letra del volumen>: \<máscara>. Si la letra del volumen falta, Kaspersky Embedded Systems Security no agregará el área de supervisión especificada.

   En el lado derecho de la ventana, la pestaña **Descripción de la regla** muestra a los usuarios de confianza y los marcadores de operaciones con archivos seleccionados para esta área de supervisión.
5. En la lista de áreas de áreas de supervisión agregadas, seleccione el área cuyas opciones desea configurar.
6. Seleccione la pestaña **Usuarios de confianza**.
7. Haga clic en el botón **Agregar**.

   Se abre la ventana estándar **Seleccionar usuarios o grupos** de Microsoft Windows.
8. Seleccione a los usuarios o los grupos de usuarios que Kaspersky Embedded Systems Security considerará de confianza para el área de supervisión seleccionada.
9. Haga clic en **Aceptar**.

   > De forma predeterminada, Kaspersky Embedded Systems Security trata a todos los usuarios que no figuran en la lista de usuarios de confianza como dudosos (consulte la sección “Acerca de las reglas de supervisión de las operaciones con archivos” en la página 375), y genera eventos críticos para ellos.
10. Seleccione la pestaña **Marcadores de operaciones con archivos**.
11. Si es necesario, realice las siguientes acciones para seleccionar varios marcadores:
    a. Seleccione la opción **Detectar las operaciones de archivos sobre la base de los siguientes marcadores**.

    b. En la lista de operaciones con archivos disponibles (consulte la sección “Acerca de las reglas de

supervisión de operaciones con archivos", en la página 375), seleccione las casillas de verificación ubicadas junto a las operaciones que desea supervisar.

> De manera predeterminada, Kaspersky Embedded Systems Security detecta todos los marcadores de operaciones con archivos, ya que está seleccionada la opción **Detectar las operaciones de archivos sobre la base de todos los marcadores reconocibles**.

12. Si desea que Kaspersky Embedded Systems Security calcule la suma de control de archivos después de que la operación se realiza, haga lo siguiente:
    a. En la sección **Cálculo de la suma de control**, seleccione la casilla de verificación **Calcular suma de control para la versión final de un archivo luego de que se haya modificado el archivo, si es posible**.

       Si la casilla se selecciona, Kaspersky Embedded Systems Security calcula la suma de control del archivo modificado, donde se detectó la operación con archivos con al menos un marcador.

       Si la operación con archivos es detectada por varios marcadores, solo se calcula la suma de control del archivo final después de que todas las modificaciones.

       Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security no calcula la suma de control para los archivos modificados.

       Ningún cálculo de la suma de control se realiza en los casos siguientes:

       - Si el archivo se volviera no disponible (por ejemplo, debido al cambio de permisos de acceso).
       - Si la operación con archivos se detecta en el archivo que se ha eliminado después.

       De forma predeterminada, la casilla está desactivada.

    b. En la lista desplegable **Calcular la suma de control que usa el algoritmo**, seleccione una de las opciones:

       - **Hash MD5**.
       - **Hash SHA256**.

13. Si es necesario, agregue áreas de supervisión excluidas al realizar los pasos siguientes:
    a. Seleccione la pestaña **Establecer exclusiones**.
    b. Seleccione la casilla de verificación **Tener en cuenta el área de supervisión excluida**.

       La casilla deshabilita el uso de exclusiones para carpetas donde las operaciones con archivos no se tienen que supervisar.

       Si la casilla se selecciona, Kaspersky Embedded Systems Security omite las áreas de alcance especificadas en la lista de exclusiones cuando la tarea del Monitor de integridad de archivos se ejecuta.

       Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security registra los eventos de todas las áreas de supervisión especificadas.

       De forma predeterminada, la casilla se desactiva y la lista de exclusión aparece vacía.

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

       Se abre la ventana estándar **Buscar carpeta** de Microsoft Windows.

    d. En la ventana que se abre, especifique el objeto que desea excluir del área de supervisión.

e. Haga clic en **Aceptar**.

f. Haga clic en el botón **Agregar**.

La carpeta especificada se añade a la lista de áreas excluidas.

> También puede añadir áreas de supervisión excluidas manualmente, usando las mismas máscaras que se usan para especificar las áreas de supervisión.

14. Haga clic en el botón **Guardar** para aplicar la nueva configuración de la regla.

Inspección de registros

Esta sección contiene la información sobre la tarea Inspección de registros y los parámetros de la tarea.

En este capítulo

Acerca de la tarea Inspección de registros

Cuando la tarea Inspección de registros se ejecuta, Kaspersky Embedded Systems Security supervisa la integridad del entorno protegido según los resultados de una inspección de registros de Eventos de Windows. La aplicación notifica al administrador cuando detecta comportamiento anormal en el sistema, que puede ser una indicación de intentos de ataques cibernéticos.

Kaspersky Embedded Systems Security considera que el evento de Windows registra e identifica incumplimientos según las reglas especificadas por un usuario o por la configuración del analizador heurístico, que se utiliza por la tarea de inspeccionar registros.

Reglas predefinidas y análisis heurístico

Puede usar la tarea Inspección de registros para supervisar el estado del sistema protegido aplicando reglas predefinidas que se basan en la heurística existente. El Analizador heurístico identifica la actividad anormal en el equipo protegido, que pueden ser pruebas de intentos de ataque. Las plantillas para identificar el comportamiento anormal se incluyen en las reglas disponibles, en la configuración de reglas predefinidas.

Se incluyen siete reglas en la lista de reglas para la tarea Inspección de registros. Puede habilitar o deshabilitar el uso de cualquiera de estas reglas. No puede eliminar las reglas existentes ni crear reglas nuevas.

Puede configurar los criterios de activación para las reglas que supervisan eventos para las siguientes operaciones:

- Detección de la fuerza bruta de la contraseña
- Detección del inicio de sesión de la red

También puede configurar exclusiones en la configuración de la tarea. El Analizador heurístico no se activa cuando un inicio de sesión es realizado por un usuario de confianza o desde una dirección IP de confianza.

> Kaspersky Embedded Systems Security no usa los parámetros heurísticos para inspeccionar registros de Windows si el analizador heurístico no es usado por la tarea. De forma predeterminada, el Analizador heurístico está habilitado.

Cuando se aplican las reglas, la aplicación registra un *Evento crítico* en el registro de tareas de Inspección de registros.

Reglas personalizadas para la tarea de Inspección de registros

Puede usar la configuración de la regla de la tarea para especificar y cambiar los criterios para desencadenar reglas al detectar los eventos seleccionados en el registro de Windows especificado. De manera predeterminada, la lista de reglas de la tarea de Inspección de registros contiene cuatro reglas. Puede habilitar y deshabilitar el uso estas reglas, eliminar reglas y modificar la configuración de la regla.

Puede configurar los siguientes criterios de activación de la regla en cada regla:

- Lista de identificadores de registro en Registro de Eventos de Windows.

  La regla se desencadena cuando un registro nuevo se crea en el Registro de Eventos de Windows, si las propiedades del evento incluyen un identificador del evento especificado para la regla. También puede agregar y eliminar identificadores para cada regla especificada.

- Origen del evento.

  Para cada regla, puede definir un subregistro del Registro de Eventos de Windows. La aplicación buscará registros con los identificadores del evento especificados solo en este subregistro. Puede seleccionar uno de los subregistros estándar (Aplicación, Seguridad o Sistema) o especificar un subregistro personalizado ingresando el nombre en el campo Selección de origen.

  > La aplicación no verifica que el subregistro especificado realmente exista en el Registro de Eventos de Windows.

Cuando la regla se desencadena, Kaspersky Embedded Systems Security registra un Evento crítico en el registro de tareas de Inspección de registros.

De manera predeterminada, la tarea Inspección de registros aplica reglas personalizadas.

> Antes de iniciar la tarea Inspección de registros, asegúrese de que la directiva de auditoría del sistema esté configurada correctamente. Consulte el artículo de Microsoft https://technet.microsoft.com/en-us/library/cc952128.aspx para obtener detalles.

Configuración predeterminada de la tarea de inspección de registros

De forma predeterminada, la tarea de Inspección de registros tiene la configuración descrita en la tabla a continuación. Puede cambiar los valores de esta configuración.

Tabla 57. Configuración de la tarea del Monitor de integridad de archivos predeterminada

Configuración	Valor predeterminado	Descripción
Aplicar reglas personalizadas para la Inspección de registros	Aplicado.	Puede habilitar, deshabilitar, agregar o modificar las reglas personalizadas.
Aplicar reglas predefinidas para la Inspección de registros	Aplicado.	Puede habilitar o deshabilitar el analizador heurístico que detecta actividad anormal en el servidor protegido.

Configuración	Valor predeterminado	Descripción
Detección de ataques de fuerza bruta	10 errores de inicio de sesión por 300 segundos.	Puede establecer el número de intentos y el período en el que se produjeron estos intentos, que se considerarán como desencadenadores para el analizador heurístico.
Inicio de sesión de red	12:00:00 a. m.	Puede indicar el inicio y el final del intervalo de tiempo durante el cual los intentos de inicio de sesión en Kaspersky Embedded Systems Security se consideraron como amenazas y como actividad anormal.
Exclusiones	No aplicado.	Puede especificar usuarios y direcciones IP que no activarán el analizador heurístico.
Programación de inicio de tareas	La primera ejecución no está programada.	Puede configurar las opciones del inicio programado de la tarea.

Gestión de reglas de inspección de registros a través del Complemento de administración

En esta sección, aprenda cómo agregar y configurar las reglas de inspección de registros a través del Complemento de administración.

En esta sección

Gestión de reglas de tarea predefinida a través del Complemento de administración

► *Realice las siguientes acciones para configurar las reglas predefinidas para la tarea Inspección de registros:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
   - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.

4. En la sección **Inspección del sistema**, haga clic en el botón **Configurar** en el bloque **Inspección de registros**.

   Se abrirá la ventana **Inspección de registros**.

5. Seleccione la pestaña **Reglas predefinidas**.
6. Seleccione o desactive la casilla de verificación **Aplicar reglas personalizadas para la inspección de registros**.

   Si esta casilla se selecciona, Kaspersky Embedded Systems Security aplica el analizador heurístico para detectar actividad anormal en el equipo protegido.

   Si esta casilla se desactiva, el analizador heurístico no se ejecutado y Kaspersky Embedded Systems Security aplica reglas predeterminadas o personalizadas de detectar la actividad anormal.

   De forma predeterminada, la casilla está activada.

Para que la tarea se ejecute, debe seleccionarse al menos una regla de inspección de registros.

7. Seleccione las reglas que desea aplicar en la lista de reglas predefinidas:
   - Hay patrones de un posible ataque de fuerza bruta en el sistema.
   - Hay patrones de un posible abuso del registro de eventos de Windows.
   - Se detectaron acciones atípicas por parte de un servicio nuevo instalado.
   - Se detectó un inicio de sesión atípico que utiliza credenciales explícitas.
   - Hay patrones de un posible ataque PAC (MS14-068) falsificado de Kerberos en el sistema.
   - Se detectaron acciones atípicas dirigidas a administradores de un grupo integrado con privilegiados.
   - Hay una actividad atípica detectada durante un inicio de sesión en la red.
8. Para configurar las reglas seleccionadas, haga clic en el botón **Configuración avanzada**.

   Se abrirá la ventana **Inspección de registros**.

9. En la sección **Detección de ataques de fuerza bruta**, configure el número de intentos y el periodo en el que se produjeron estos intentos, que se considerarán como desencadenadores para el analizador heurístico.
10. En la sección **Detección de inicio de sesión en la red**, indique el inicio y el final del intervalo de tiempo durante el cual los intentos de inicio de sesión en Kaspersky Embedded Systems Security se consideraron como amenazas y como actividad anormal.
11. Seleccione la pestaña **Exclusiones**.

12. Realice las siguientes acciones para agregar a usuarios de confianza:
    a. Haga clic en el botón **Examinar**.
    b. Seleccione a un usuario.
    c. Haga clic en **Aceptar**.

    Un usuario seleccionado se añade a la lista de usuarios de confianza.
13. Realice las siguientes acciones para agregar Direcciones IP de confianza:
    a. Escriba la Dirección IP.
    b. Haga clic en el botón **Agregar**.
14. Una Dirección IP indicada se añade a la lista de Direcciones IP de confianza.
15. En la pestaña **Administración de la tarea**, configure la programación de inicio de tareas (consulte la sección “Configuración de las opciones de programación de inicio de tareas”, en la página 128).
16. Haga clic en **Aceptar**.

La configuración de la tarea Inspección de registros se guardó.

Cómo agregar reglas de Inspección de registros a través del Complemento de administración

► *Realice las siguientes acciones para agregar y configurar una nueva regla personalizada de Inspección de registros:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea ajustar la configuración de la aplicación.
3. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
    - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas” en la página 113).
    - Para configurar una solicitud para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación del Kaspersky Security Center” en la página 117).

    > Si se aplica una directiva activa de Kaspersky Security Center a un dispositivo, y esta directiva bloquea los cambios de la configuración de la aplicación, entonces no se puede editar esta configuración en la ventana **Configuración de la aplicación**.
4. En la sección **Inspección del sistema**, haga clic en el botón **Configurar** en el bloque **Inspección de registros**.

    Se abrirá la ventana **Inspección de registros**.
5. En la pestaña **Reglas personalizadas**, seleccione o desmarque la casilla de verificación **Aplicar reglas personalizadas para la inspección de registros**.

    Si la casilla está seleccionada, Kaspersky Embedded Systems Security aplica reglas personalizadas para la Inspección de registros según cada configuración de reglas.

Puede agregar, eliminar o configurar reglas de Inspección de registros.

Si la casilla está desactivada, no puede agregar ni modificar las reglas personalizadas. Kaspersky Embedded Systems Security aplica la configuración de reglas predeterminada.

De forma predeterminada, la casilla está activada. Solo la regla Detección de aplicaciones emergentes está activa.

Puede controlar si las reglas predeterminadas se aplican para la Inspección de registros. Seleccione las casillas correspondientes a las reglas desea aplicar a la Inspección de registros.

6. Para agregar una nueva regla personalizada, haga clic en el botón **Agregar**.

   Se abre la ventana **Reglas de inspección de registros**.

7. En la sección **General**, ingrese la siguiente información sobre la regla nueva:

   - **Nombre de regla**
   - **Origen**

     Seleccione un registro de fuentes para usar los eventos registrados para el análisis. Los siguientes tipos de registros de eventos de Windows están disponibles:

     - Aplicación
     - Seguridad
     - Sistema

     Puede agregar un nuevo registro personalizado ingresando el nombre del registro en el campo **Origen**.

8. En la sección **ID de eventos desencadenadores**, especifique los Id. de los elementos que activarán la regla tras la detección:

   a. Escriba el valor numérico de un ID.

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

      El ID de la regla seleccionado se añade a la lista. Puede agregar un número ilimitado de identificadores para cada regla.

   c. Haga clic en **Aceptar**.

   La regla de inspección de registros se añade a la lista de reglas.

Gestión de reglas de Inspección de registros a través de la Consola de la aplicación

En esta sección, aprenda cómo agregar y configurar reglas de Inspección de registros a través de la Consola de la aplicación.

En esta sección

Gestión de reglas de tarea predefinida a través de la Consola de la aplicación

► *Realice las siguientes acciones para configurar el analizador heurístico para la tarea Inspección de registros:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Inspección del sistema**.
2. Seleccione el nodo secundario **Inspección de registros**.
3. Haga clic en el vínculo **Propiedades** en el panel de detalles del nodo **Inspección de registros**.

   Se abre la ventana **Configuración de tareas**.
4. Seleccione la pestaña **Reglas predefinidas**.
5. Seleccione o desactive la casilla de verificación **Aplicar reglas personalizadas para la inspección de registros**.

   Si esta casilla se selecciona, Kaspersky Embedded Systems Security aplica el analizador heurístico para detectar actividad anormal en el equipo protegido.

   Si esta casilla se desactiva, el analizador heurístico no se ejecutado y Kaspersky Embedded Systems Security aplica reglas predeterminadas o personalizadas de detectar la actividad anormal.

   De forma predeterminada, la casilla está activada.

   Para que la tarea se ejecute, debe seleccionarse al menos una regla de inspección de registros.
6. Seleccione las reglas que desea aplicar en la lista de reglas predefinidas:
   - Hay patrones de un posible ataque de fuerza bruta en el sistema.
   - Hay patrones de un posible abuso del registro de eventos de Windows.
   - Se detectaron acciones atípicas por parte de un servicio nuevo instalado.
   - Se detectó un inicio de sesión atípico que utiliza credenciales explícitas.
   - Hay patrones de un posible ataque PAC (MS14-068) falsificado de Kerberos en el sistema.
   - Se detectaron acciones atípicas dirigidas a administradores de un grupo integrado con privilegiados.
   - Hay una actividad atípica detectada durante un inicio de sesión en la red.

7. Para configurar las reglas seleccionadas, vaya a la pestaña **Extendido**.
8. En la opción **Detección de ataques de fuerza bruta**, establezca el número de intentos y el periodo en el que se produjeron estos intentos, que se considerarán como desencadenadores para el análisis heurístico.
9. En la sección **Inicio de sesión en la red**, indique el inicio y el final del intervalo de tiempo durante el cual los intentos de inicio de sesión en Kaspersky Embedded Systems Security se consideraron como amenazas y como actividad anormal.
10. Seleccione la pestaña **Exclusiones**.
11. Realice las siguientes acciones para agregar a usuarios de confianza:
    a. Haga clic en el botón **Examinar**.
    b. Seleccione a un usuario.
    c. Haga clic en **Aceptar**.

    Un usuario seleccionado se añade a la lista de usuarios de confianza.
12. Realice las siguientes acciones para agregar Direcciones IP de confianza:
    a. Escriba la Dirección IP.
    b. Haga clic en el botón **Agregar**.

    Una Dirección IP indicada se añade a la lista de Direcciones IP de confianza.
13. Seleccione las pestañas **Programación** y **Avanzado** para configurar la programación de inicio de tareas.
14. Haga clic en **Aceptar**.

    La configuración de la tarea Inspección de registros se guardó.

Configuración de las reglas de inspección de registros

Realice las siguientes acciones para agregar y configurar una nueva regla personalizada de Inspección de registros:

1. En el árbol de la Consola de la aplicación, expanda el nodo **Inspección del sistema**.
2. Seleccione el nodo secundario **Inspección de registros**.
3. En el panel de detalles del nodo **Inspección de registros**, haga clic en el vínculo **Reglas de inspección de registros**.

   Se abre la ventana **Reglas de inspección de registros**.
4. Seleccione o desactive la casilla **Aplicar reglas personalizadas para la inspección de registros**.

   Si la casilla está seleccionada, Kaspersky Embedded Systems Security aplica reglas personalizadas para la Inspección de registros según cada configuración de reglas. Puede agregar, eliminar o configurar reglas de Inspección de registros.

   Si la casilla está desactivada, no puede agregar ni modificar las reglas personalizadas. Kaspersky Embedded Systems Security aplica la configuración de reglas predeterminada.

   De forma predeterminada, la casilla está activada. Solo la regla Detección de aplicaciones emergentes está activa.

Puede controlar si las reglas predefinidas se aplican para la tarea Inspección de registros. Seleccione las casillas correspondientes a las reglas desea aplicar a la Inspección de registros.

5. Para crear una nueva regla personalizada, haga lo siguiente:
   a. Introduzca el nombre de la nueva regla.
   b. Haga clic en el botón **Agregar**.

      La regla creada se agrega a la lista de reglas generales.
6. Para configurar cualquier regla, siga estos pasos:
   a. Haga clic con el botón izquierdo del ratón para seleccionar una regla de la lista.

      En el lado derecho de la ventana, la pestaña **Descripción** muestra información general sobre la regla.

      > La descripción de la nueva regla está en blanco.

   b. Seleccione la pestaña **Descripción de la regla**.
   c. En la sección **General**, edite el nombre de la regla, si fuera necesario.
   d. Seleccione la **Origen**.
7. En la sección **Identificadores de eventos**, especifique los Id. del elemento que desencadenarán la regla tras la detección:
   a. Escriba el valor numérico de un ID.
   b. Haga clic en el botón **Agregar**.

      El ID de la regla seleccionado se añade a la lista. Puede agregar un número ilimitado de identificadores para cada regla.
   c. Haga clic en el botón **Guardar**.

      Las reglas de inspección de registros configuradas se aplicarán.

Análisis a pedido

Esta sección proporciona la información sobre las tareas de Análisis a pedido e instrucciones de la configuración de los ajustes de la tarea Análisis a pedido y ajustes de seguridad en el equipo protegido.

En este capítulo

Acerca de las tareas de Análisis a pedido

Kaspersky Embedded Systems Security analiza la zona especificada en busca de virus y otras amenazas de seguridad informática. Kaspersky Embedded Systems Security analiza archivos de equipos y RAM, así como objetos de ejecución automática.

Kaspersky Embedded Systems Security proporciona las siguientes tareas del sistema de Análisis a pedido:

- La tarea Análisis al inicio del sistema operativo se realiza cada vez que se inicia Kaspersky Embedded Systems Security. Kaspersky Embedded Systems Security analiza los sectores de inicio y los registros de inicio maestro de los discos duros y las unidades extraíbles, la memoria del sistema y la memoria de los procesos. Cada vez que Kaspersky Embedded Systems Security ejecuta la tarea, crea una copia de los sectores de inicio no infectados. Si en el próximo inicio de la tarea se detecta una amenaza en esos sectores, los reemplaza con la copia de seguridad.
- De forma predeterminada, la tarea de Análisis de áreas críticas se realiza cada semana según la programación. Kaspersky Embedded Systems Security analiza los objetos ubicados en las áreas críticas del sistema operativo: objetos de ejecución automática, sectores de inicio y registros de inicio maestro de discos duros y unidades extraíbles, memoria del sistema y memoria de los procesos. La aplicación analiza los archivos que se encuentran en las carpetas del sistema, por ejemplo, en %windir%\system32. Kaspersky Embedded Systems Security aplica la configuración de seguridad, cuyos valores equivalen al Nivel recomendado (consulte la sección “Acerca de los niveles de seguridad predefinidos para tareas de Análisis a pedido” en la página 402). Puede modificar la configuración de la tarea de Análisis de áreas críticas.

- La tarea de Análisis de archivos en cuarentena se ejecuta de manera predeterminada según la programación después de cada actualización de las bases de datos. El alcance la tarea de Análisis de archivos en cuarentena no se puede modificar.
- La tarea Control de integridad de la aplicación se realiza a diario. Proporciona la opción de comprobar módulos de Kaspersky Embedded Systems Security en busca de daños o modificaciones. Se comprueba la carpeta de instalación de la aplicación. Las estadísticas de ejecución de tareas contienen información sobre el número de módulos comprobados y dañados. Los valores de la configuración de tarea están definidos de forma predeterminada y no se pueden modificar. La configuración de la programación de inicio de tareas se puede modificar.

Además, puede crear tareas de Análisis a pedido personalizadas, por ejemplo, una tarea para analizar las carpetas compartidas en el equipo.

Kaspersky Embedded Systems Security puede ejecutar varias tareas de Análisis a pedido de manera simultánea.

Acerca del área del análisis

Puede configurar el área del análisis para las tareas de Análisis al inicio del sistema operativo y Análisis de áreas críticas, y para las tareas de Análisis a pedido personalizadas.

De forma predeterminada, las tareas de Análisis a pedido analizan todos los objetos del sistema de archivos del equipo. Si no hay requisitos de seguridad para analizar todos los objetos del sistema de archivos, puede limitar el análisis al área del análisis.

En la Consola de la aplicación, el área del análisis se muestra como un árbol o como una lista de recursos de archivos del equipo que Kaspersky Embedded Systems Security puede controlar. De forma predeterminada, los recursos de archivos en red del equipo protegido se muestran en un modo de vista de lista.

► *Para ver recursos de archivos en red en el modo de vista de árbol,*

abra la lista desplegable en el sector izquierdo superior de la ventana **Configuración del área de análisis** y seleccione **Vista de árbol**.

Los nodos se muestran en una visualización en forma de lista o en un modo de visualización en forma de árbol de los recursos del archivo del equipo de la siguiente manera:

 El nodo se incluye en el área del análisis.

 El nodo se excluye del área del análisis.

 Al menos uno de los nodos secundarios de este nodo se excluye del área del análisis o la configuración de seguridad de los nodos secundarios difiere de la de este nodo (solo para el modo de vista de árbol).

El icono  se muestra si están seleccionados todos los nodos secundarios, pero no el principal. En este caso, los cambios en la composición de los archivos y las carpetas del nodo principal se ignoran automáticamente cuando se está modificando el área del análisis para el subnodo seleccionado.

Los nombres de los nodos virtuales del área del análisis se muestran en letras azules.

Áreas de análisis predefinidas

El árbol o la lista de recursos del archivo del equipo para la tarea de Análisis a pedido seleccionada se muestran en la pestaña **Configuración del área de análisis**.

El árbol o la lista de recursos de archivos muestran los nodos a los cuales tiene acceso de lectura según la configuración de seguridad de Microsoft Windows.

Kaspersky Embedded Systems Security contiene las áreas de análisis predefinidas siguientes:

- **Mi equipo**. Kaspersky Embedded Systems Security analiza todo el equipo.
- **Discos duros locales**. Kaspersky Embedded Systems Security analiza objetos en los discos duros del equipo. Todos los discos duros, discos, carpetas o archivos individuales se pueden incluir en el área del análisis o excluir de él.
- **Unidades extraíbles**. Kaspersky Embedded Systems Security analiza archivos en dispositivos externos, por ejemplo, unidades USB o CD. Todas las unidades extraíbles, discos, carpetas o archivos individuales pueden incluirse en el área del análisis o excluirse de ella.
- **Red**. Para agregar los archivos o las carpetas de red al área del análisis, especifique su ruta en formato UNC (convención de nomenclatura universal). La cuenta usada para iniciar la tarea debe tener permisos de acceso para los archivos y las carpetas de red que se agregan. De forma predeterminada, las tareas de Análisis a pedido se ejecutan en la cuenta de sistema.

  Las unidades de red conectadas tampoco se mostrarán en el árbol de recursos de archivos del equipo. Para incluir objetos de unidades de red en el área del análisis, especifique la ruta a la carpeta que corresponde a esta unidad de red en formato UNC.

- **Memoria del sistema**. Kaspersky Embedded Systems Security analiza los módulos y archivos ejecutables de los procesos que se ejecutan en el sistema operativo cuando se inicia el análisis.
- **Objetos de inicio**. Kaspersky Embedded Systems Security analiza objetos referidos por claves de registro y archivos de configuración, por ejemplo WIN.INI o SYSTEM.INI, así como los módulos de la aplicación que se inician automáticamente en el inicio del equipo.
- **Carpetas compartidas**. Puede incluir carpetas compartidas del equipo protegido en el área del análisis.
- **Unidades virtuales**. Las unidades, archivos y carpetas dinámicos que se conectan al equipo se pueden incluir en el área del análisis, por ejemplo, unidades de clústeres comunes.

  Las unidades virtuales creadas mediante un comando SUBST no se muestran en el árbol de recursos de archivo del equipo de la Consola de la aplicación. Para analizar objetos en una unidad virtual, incluya la carpeta del equipo con la que se asocia esta unidad virtual en el área del análisis.

De forma predeterminada, puede ver y configurar las áreas de análisis predefinidas en el árbol de recursos de archivos en red; y también puede agregar áreas predefinidas a la lista de recursos de archivos en red durante su formación en la configuración del área de análisis.

De forma predeterminada, las tareas de Análisis a pedido se ejecutan según las diferentes áreas:

- Tarea de Análisis al inicio del sistema operativo:
  - **Discos duros locales**
  - **Unidades extraíbles**
  - **Memoria del sistema**
- Análisis de áreas críticas:
  - **Discos duros locales** (excluidas las carpetas de Windows)
  - **Unidades extraíbles**
  - **Memoria del sistema**
  - **Objetos de inicio**
- Otras tareas:
  - **Discos duros locales** (excluidas las carpetas de Windows)
  - **Unidades extraíbles**
  - **Memoria del sistema**
  - **Objetos de inicio**
  - **Carpetas compartidas**

Análisis de archivos almacenados en la nube

Acerca de los archivos en la nube

Kaspersky Embedded Systems Security puede interactuar con archivos en la nube de Microsoft OneDrive. La aplicación admite la nueva función archivos a pedido de OneDrive.

> Kaspersky Embedded Systems Security no admite otros depósitos en la nube.

OneDrive Files On-Demand ayuda a acceder a todos los archivos en OneDrive sin necesidad de descargarlos todos y utilizar espacio de almacenamiento en el dispositivo. Puede descargar archivos en el disco duro cuando lo necesite.

Cuando la función OneDrive Files On-Demand está activada, ve los iconos de estado junto a cada archivo en la columna **Estado** en el Explorador de archivos. Cada archivo tiene uno de los siguientes estados:

 Este icono de estado indica que el archivo *solo está disponible en línea*. Los archivos que están solo en línea no se almacenan físicamente en el disco duro. No puede abrir archivos que están solo en línea cuando su dispositivo no está conectado a Internet.

 Este icono de estado indica que un archivo *está disponible localmente*. Esto sucede cuando abre un archivo solo en línea y lo descarga a su dispositivo. Puede abrir un archivo disponible localmente en cualquier momento, incluso sin acceso a Internet. Para liberar espacio, puede cambiar el archivo nuevamente a  solo en línea.

 Este icono de estado indica que un archivo *está almacenado en el disco duro y siempre está disponible*.

Análisis de archivos en la nube

Kaspersky Embedded Systems Security solo puede analizar archivos en la nube que están almacenados localmente en un equipo protegido. Estos archivos de OneDrive deben tener los estados  y  . Los archivos  se omiten durante el análisis, ya que no están ubicados físicamente en el equipo protegido.

Kaspersky Embedded Systems Security no descarga automáticamente los archivos  de la nube durante el análisis, aunque estén incluidos en el área del análisis.

Varias tareas de Kaspersky Embedded Systems Security procesan los archivos en la nube en distintas situaciones según el tipo de tarea:

- Análisis de archivos en la nube en tiempo real: puede agregar carpetas que contienen archivos en la nube área de la tarea Protección de archivos en tiempo real. El archivo se analiza cuando el usuario accede a él. Si el usuario accede al archivo  , se descarga para estar disponible localmente y su estado cambia a  . Esto permite que la tarea de Protección de archivos en tiempo real procese el archivo.
- Análisis a pedido de archivos en la nube: puede agregar carpetas que contienen archivos en la nube al área de la tarea Análisis a pedido. La tarea analiza archivos con los estados  y  . Si se encuentra algún archivo  en el área, se omitirá durante el análisis, y se registrará un evento informativo en el registro de tareas para indicar que el archivo analizado solo es un marcador de posición de un archivo en la nube y no existe en un disco local.
- Generación y uso de reglas de Control de aplicaciones: puede crear reglas de autorización y de denegación de archivos  y  con la tarea del Generador de reglas para Control de inicio de aplicaciones. La tarea Control de inicio de aplicaciones aplica el principio de denegación predeterminada y las reglas creadas para procesar y bloquear archivos en la nube.

  La tarea Control de inicio de aplicaciones bloquea el inicio de todos los archivos en la nube más allá de su estado. Los archivos  no se incluyen en el área de generación de reglas que realiza la aplicación, ya que no están presentes físicamente en un disco duro. Como no puede crearse ninguna regla para estos archivos, están sujetos al principio de denegación predeterminada.

Cuando se detecta una amenaza en un archivo de OneDrive en la nube, la aplicación realiza la acción especificada en la configuración de la tarea que lleva a cabo el análisis. De esta manera, se puede realizar una copia de seguridad del archivo, o bien se lo puede eliminar, desinfectar o mover a la cuarentena.

Los cambios en los archivos locales se sincronizan con las copias almacenadas en OneDrive de acuerdo con los principios descritos en la documentación de Microsoft OneDrive.

Configuración de seguridad del nodo seleccionado en tareas de Análisis a pedido

En la tarea Análisis a pedido, los valores predeterminados de la configuración de seguridad se pueden modificar si

se configuran como valores comunes para todo el alcance de la protección o del análisis, o como valores diferentes para los diferentes nodos o elementos en la lista o el árbol de recursos de archivos del equipo.

La configuración de seguridad para el nodo principal seleccionado se aplica automáticamente a todos los nodos secundarios. La configuración de seguridad del nodo principal no se aplica a nodos secundarios que se configuran por separado.

La configuración de un área del análisis o alcance de la protección seleccionada se puede realizar mediante uno de los métodos siguientes:

- Seleccione uno de los tres niveles de seguridad predefinidos (**Máximo Rendimiento**, **Recomendado** o **Máxima Protección**).
- Cambie manualmente la configuración de seguridad para los nodos o elementos seleccionados en el árbol o en la lista de los recursos de archivos del equipo (el nivel de seguridad cambia a **Personalizado**).

Es posible guardar un conjunto de opciones de configuración de seguridad en una plantilla a fin de aplicarlo más tarde a otros nodos.

Acerca de los niveles de seguridad predefinidos para tareas de Análisis a pedido

La configuración de seguridad de **Usar la tecnología iChecker**, **Usar la tecnología iSwift**, **Usar el analizador heurístico** y **Comprobar si el archivo está firmado por Microsoft** no se incluyen en la configuración de los niveles de seguridad predefinidos. Si se modifican los estados de las configuraciones como **Usar la tecnología iChecker**, **Usar la tecnología iSwift**, **Usar el analizador heurístico** y **Comprobar si el archivo está firmado por Microsoft**, el nivel de seguridad predefinido seleccionado no cambiará.

Se puede aplicar uno de los tres siguientes niveles de seguridad predefinidos para un nodo seleccionado en el árbol de recursos de archivos del equipo: **Máximo Rendimiento**, **Recomendado** y **Máxima Protección**. Cada uno de estos niveles contiene su propio conjunto de configuraciones de seguridad predefinidas (consulte la tabla a continuación).

Máximo Rendimiento

El nivel de seguridad **Máximo Rendimiento** se recomienda si, además del uso de Kaspersky Embedded Systems Security en los equipos, existen medidas adicionales de seguridad del equipo en la red, por ejemplo, si hay firewalls y directivas de seguridad existentes.

Recomendado

El nivel de seguridad **Recomendado** garantiza una óptima combinación de protección e impacto en el rendimiento de los equipos protegidos. Este nivel es recomendado por los expertos de Kaspersky Lab como suficiente para proteger equipos en la mayoría de las redes empresariales. El nivel de seguridad **Recomendado** está configurado de manera predeterminada.

Máxima Protección

Se recomienda el nivel de seguridad **Máxima Protección** si la red de la organización ha elevado los requisitos de seguridad del equipo.

Tabla 58. Niveles de seguridad predefinidos y los valores de configuración de seguridad correspondientes

Opciones	Nivel de seguridad

Opciones	Nivel de seguridad		
	Máximo Rendimiento	Recomendado	Máxima Protección
Analizar objetos	Por formato	Todos los objetos	Todos los objetos
Analizar solo los archivos nuevos y modificados	Habilitado	Deshabilitado	Deshabilitado
Acción que se realizará con los objetos infectados y otros objetos	Desinfectar. Eliminar si falla la desinfección	Ejecutar la acción recomendada (Desinfectar; eliminar si falla la desinfección)	Desinfectar. Eliminar si falla la desinfección
Acción que se realizará con los objetos probablemente infectados	Cuarentena	Ejecutar la acción recomendada (Cuarentena)	Cuarentena
Excluir archivos	No	No	No
No detectar	No	No	No
Detener el análisis si demora más de (seg.)	60 segundos.	No	No
Omitir objetos compuestos de más de (MB)	8 MB	No	No
Analizar secuencias alternativas de NTFS	Sí	Sí	Sí
Analizar sectores de inicio del disco y MBR	Sí	Sí	Sí
Análisis de objetos compuestos	• Archivos SFX* • Objetos empaquetados* • Objetos OLE integrados* * Sólo objetos nuevos y modificados	• Archivos* • Archivos SFX* • Objetos empaquetados* • Objetos OLE integrados* * Todos los objetos	• Archivos* • Archivos SFX* • Bases de datos de correo electrónico* • Correo sin formato* • Objetos empaquetados* • Objetos OLE integrados* * Todos los objetos

Acerca del Análisis de unidades extraíbles

Puede configurar el análisis de discos extraíbles conectados al equipo protegido mediante el puerto USB.

Kaspersky Embedded Systems Security analiza un disco extraíble mediante la tarea Análisis a pedido. La aplicación crea automáticamente una nueva tarea de Análisis a pedido cuando la unidad extraíble está conectada y la suprime después de que se completa el análisis. La tarea creada se realiza con el nivel de seguridad predefinido determinado para el análisis de unidades extraíbles. No puede configurar los valores de la tarea

temporal de Análisis a pedido.

Si instaló Kaspersky Embedded Systems Security sin bases de datos antivirus, el análisis de unidades extraíbles no estará disponible.

Kaspersky Embedded Systems Security analiza un disco extraíble mediante la tarea Análisis a pedido. La aplicación crea automáticamente una nueva tarea de Análisis a pedido cuando la unidad extraíble está conectada y la suprime después de que se completa el análisis. La tarea creada se realiza con el nivel de seguridad predefinido determinado para el análisis de unidades extraíbles. No puede configurar los valores de la tarea temporal de Análisis a pedido.

Los análisis de Kaspersky Embedded Systems Security conectaron discos USB extraíbles cuando se registran como dispositivos de almacenamiento USB en el sistema operativo. La aplicación no analiza una unidad extraíble si la conexión está bloqueada por la tarea Control de dispositivos. La aplicación no analiza dispositivos móviles conectados a MTP.

Kaspersky Embedded Systems Security permite el acceso a las unidades extraíbles durante el análisis.

Los resultados de análisis para cada unidad extraíble están disponibles en el registro para la tarea Análisis a pedido creada al conectar la unidad extraíble.

Puede cambiar las configuraciones predeterminadas de la tarea Monitor de Integridad de archivos (consulte la tabla a continuación).

Tabla 59. Configuración de Análisis de unidades extraíbles

Configuración	Valor predeterminado	Descripción
Analizar discos extraíbles al conectarlos via USB	La casilla se desactiva.	Puede activar o desactivar el análisis de las unidades extraíbles después de conectarlas al equipo protegido por USB.
Analizar las unidades extraíbles si el volumen de los datos almacenados no excede (MB)	1024 MB	Puede reducir el área del componente si configura el volumen máximo de datos del disco analizado. Kaspersky Embedded Systems Security no realiza análisis de unidades extraíbles si el volumen de datos almacenados excede el valor especificado.
Analizar con nivel de seguridad	Máxima protección	Puede configurar las tareas creadas de Análisis a pedido a través de uno de los tres niveles de seguridad: • **Máxima Protección** • **Recomendado** • **Máximo Rendimiento** El algoritmo usado cuando se detectaron objetos infectados, posiblemente infectados y otros objetos, así como otras configuraciones de análisis para cada nivel de seguridad, equivalen a los niveles de seguridad predefinidos en las tareas Análisis a pedido.

Configuración de tareas de Análisis a pedido

De manera predeterminada, las tareas de Análisis a pedido tienen la descripción de la configuración en la tabla de arriba. Puede configurar tareas de Análisis a pedido de sistema y de usuario.

Tabla 60. Configuración de tareas de Análisis a pedido

Configuración	Valor	Descripción
Área del análisis	Aplicado en tareas de sistema y personalizadas: • **Análisis al inicio del sistema operativo**: el servidor completo, excluidas las carpetas compartidas y los objetos de ejecución automática. • **Análisis de áreas críticas**: el servidor completo, excluidas las carpetas compartidas y determinados archivos del sistema operativo. • Tareas de **Análisis a pedido** personalizadas: el servidor completo.	Se puede cambiar el área del análisis. El alcance del análisis no se puede configurar para las tareas de sistema de **Análisis de archivos en cuarentena** y **Control de integridad de la aplicación**.

Configuración	Valor	Descripción
Configuración de seguridad	La configuración común para toda el área del análisis corresponde al nivel de seguridad **Recomendado**.	Para los nodos seleccionados en la lista o el árbol de recursos de archivos del equipo, puede realizar lo siguiente: • Seleccionar un nivel de seguridad predefinido diferente • Cambiar manualmente la configuración de seguridad Puede guardar una configuración de seguridad definida para un nodo seleccionado como una plantilla para usarla más tarde en un nodo diferente.
Usar el analizador heurístico	Se utiliza con el nivel de análisis **Medio** para tareas de Análisis de áreas críticas, Análisis al inicio del sistema operativo y tareas personalizadas. Se utiliza con el nivel de análisis **Profundo** para la tarea de Análisis de archivos en cuarentena.	Se puede habilitar o deshabilitar el Analizador heurístico y se puede configurar el nivel de análisis. El nivel de la tarea de Análisis de archivos en cuarentena no se puede configurar. El Analizador heurístico no se usa en la tarea de Control de integridad de la aplicación.
Aplicar la Zona de confianza	Aplicado (no se aplicó a una tarea de Análisis de archivos en cuarentena)	Lista general de exclusiones que se puede utilizar en tareas seleccionadas.
Usar KSN para análisis	Aplicado	Puede mejorar la protección del servidor con la infraestructura de Kaspersky Security Network de servicios en la nube.
Configuración del inicio de tareas con permisos	La tarea se inicia con una cuenta de sistema.	Puede modificar la configuración del inicio con permisos de la cuenta para todas las tareas de Análisis a pedido de sistema o de usuario, excepto las tareas de Análisis de archivos en cuarentena y Control de integridad de la aplicación.
Ejecutar tarea en segundo plano (prioridad baja)	No aplicado	Puede configurar el nivel de prioridad de las tareas de Análisis a pedido.
Programación de inicio de tareas	Aplicado en tareas de sistema: • Análisis al inicio del sistema operativo: **Al inicio de la aplicación** • Análisis de áreas críticas: **Semanal** • Análisis de archivos en cuarentena: **Tras la actualización de bases de datos de la aplicación** • Control de integridad de la aplicación: **Diaria** No se utiliza en tareas personalizadas recientemente.	Puede configurar las opciones del inicio programado de la tarea.

Configuración	Valor	Descripción
Registro de ejecución del análisis y actualización del estado de protección del servidor	El estado de protección del servidor se actualiza cada semana después de la realización del Análisis de áreas críticas.	Puede configurar las opciones para registrar la ejecución del Análisis de áreas críticas de los siguientes modos: • Modificando la configuración de la programación de inicio de la tarea de Análisis de áreas críticas. • Modificando el área del análisis de la tarea de Análisis de áreas críticas. • Creando tareas de Análisis a pedido de usuario.

Gestión de tareas de Análisis a pedido a través del Complemento de administración

En esta sección, aprenderá a navegar la interfaz del Complemento de administración y ajustar la configuración de la tarea para uno o todos los equipos en la red.

En esta sección

Navegación

Sepa cómo navegar a la configuración de la tarea requerida a través de la interfaz.

En esta sección

Cómo abrir el asistente de la tarea de Análisis a pedido

► *Para empezar a crear una tarea nueva de Análisis a pedido personalizada:*

1. Para crear una tarea local:
   a. Expanda el nodo **Dispositivos administrados** en la Consola de administración de Kaspersky Security Center.
   b. Seleccione el grupo de administración al cual pertenece el equipo.
   c. En el panel de detalles, en la pestaña **Dispositivos**, abra el menú contextual para el servidor protegido.
   d. Seleccione la opción del menú **Propiedades**.
   e. En la ventana que se abre, haga clic en el botón **Agregar** en la sección **Tareas**.

   Se abre la ventana **Nuevo asistente de tarea** .
2. Para crear una tarea de grupo:
   a. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
   b. Seleccione el grupo de administración para el cual desea crear una tarea.
   c. Abra la pestaña **Tareas**.
   d. Haga clic en el botón **Crear una tarea** .

   Se abre la ventana **Nuevo asistente de tarea** .
3. Para crear una tarea para un conjunto personalizado de equipos:
   a. En el nodo **Selecciones de dispositivos** en el árbol de la Consola de administración de Kaspersky Security Center, haga clic en el botón **Ejecutar selección** para realizar una selección de dispositivos.
   b. Abra la pestaña **Resultados de selección *nombre de selección***.
   c. En la lista desplegable **Realizar selección**, seleccione la opción **Crear una tarea para un resultado de selección** .

   Se abre la ventana **Nuevo asistente de tarea** .
4. Seleccione la tarea **Análisis a pedido** en la lista de tareas disponibles para Kaspersky Embedded Systems Security.
5. Haga clic en **Siguiente**.

   Se abre la ventana **Configuración**.

Ajuste la configuración de la tarea como sea necesario.

► *Para configurar una tarea de Análisis a pedido existente,*

haga doble clic en el nombre de la tarea en la lista de tareas de Kaspersky Security Center.

Se abre la ventana **Propiedades:** Se abre la ventana **Análisis a pedido**.

Cómo abrir las propiedades de la tarea de Análisis a pedido

► *Para abrir las propiedades de la aplicación para la tarea de Análisis a pedido en un solo equipo:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración al cual pertenece el equipo protegido.
3. Seleccione la pestaña **Dispositivos** .
4. Haga doble clic en el nombre del equipo para el cual desea configurar el área de análisis.

   Se abre la ventana **Propiedades: <Nombre del equipo>**.
5. Seleccione la sección **Tareas**.
6. En la lista de tareas creadas para el dispositivo, seleccione la tarea de Análisis a pedido que creó.
7. Haga clic en el botón **Propiedades**.

   Se abre la ventana **Propiedades:** Se abre la ventana **Análisis a pedido**.

Ajuste la configuración de la tarea como sea necesario.

Creación de una tarea de Análisis a pedido

► *Para crear una tarea de Análisis a pedido personalizada:*

1. Abra la ventana **Configuración** (consulte la sección "**Cómo abrir el asistente de la tarea de Análisis a pedido**" en la página 408) en el **Nuevo asistente de tarea**.
2. Seleccione el **Método de creación de la tarea** requerido.
3. Haga clic en **Siguiente**.
4. Cree un área del análisis en la ventana **Área del análisis**:

   De manera predeterminada, el área del análisis incluye áreas críticas del equipo. Las áreas del análisis están marcadas en la tabla con el icono Las áreas del análisis excluidas están marcadas con el icono en la tabla.
   Puede cambiar el área del análisis: agregar áreas del análisis predefinidas, discos, carpetas, objetos de red y archivos, y asignar la configuración de seguridad específica para cada área agregada.

   - Para excluir todas las áreas críticas del análisis, abra el menú contextual en cada una de las líneas y seleccione la opción **Eliminar área**.
   - Para incluir un área del análisis predeterminada, disco, carpeta, objeto de red o archivo en el área del análisis:

     a. Haga clic con el botón derecho en la tabla **Área del análisis** y seleccione **Agregar área**, o bien haga clic en el botón **Agregar**.

     b. En la ventana **Agregar objetos al área de análisis**, seleccione el área predefinida en la lista **Área predefinida**, especifique el disco, la carpeta, el objeto de red o el archivo en el equipo o en otro equipo en red y haga clic en el botón **Aceptar**.
   - Para excluir subcarpetas o archivos del análisis, seleccione la carpeta (o el disco) agregado en la

ventana **Área del análisis** del asistente:

a. Abra el menú contextual y seleccione la opción **Configurar**.

b. Haga clic en el botón **Configurar** en la ventana **Nivel de seguridad**.

c. En la pestaña **General** de la ventana **Configuración del análisis a pedido**, cancele la selección de las casillas de verificación **Subcarpetas** y **Subarchivos**.

- Para cambiar la configuración de seguridad del área del análisis:

  a. Abra el menú contextual en el análisis cuya configuración desea definir y seleccione **Configurar**.

  b. En la ventana **Configuración del análisis a pedido**, seleccione uno de los niveles de seguridad predefinidos o haga clic en el botón **Configurar** para definir la configuración de seguridad manualmente.

  Las opciones de seguridad se configuran de la misma manera que en la tarea Protección de archivos en tiempo real (consulte la sección “Configuración manual de las opciones de seguridad” en la página 246).

- Para omitir objetos integrados en el área del análisis agregada:

  a. Abra el menú contextual en la tabla **Área del análisis** y seleccione **Agregar exclusión**.

  b. Especifique los objetos que desea excluir: seleccione el área predefinida en la lista **Área predefinida**, especifique el disco del equipo, la carpeta, el objeto de red o el archivo en el equipo o en otro equipo de la red.

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

5. En la ventana **Opciones**, configure el analizador heurístico y la integración con los demás componentes:

   - Configure la aplicación del analizador heurístico (consulte la sección "Configuración del Analizador heurístico e integración con otros componentes de la aplicación" en la página 242).
   - Seleccione la casilla de verificación **Aplicar la Zona de confianza** si quiere excluir objetos agregados en la lista de Zona de confianza del área del análisis de la tarea.

     Esta casilla de verificación habilita y deshabilita el uso de la Zona de confianza para una tarea.

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security agrega operaciones del archivo de procesos de confianza a las exclusiones de análisis configuradas en la tarea.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security ignora las operaciones del archivo de procesos de confianza al formar el alcance de la protección para la tarea.

     De forma predeterminada, la casilla está activada.

   - Seleccione la casilla de verificación **Usar KSN para análisis** si desea usar los servicios en la nube de Kaspersky Security Network para la tarea.

     Esta casilla de verificación habilita y deshabilita el uso de servicios en la nube de Kaspersky Security Network (KSN) en la tarea.

     Si la casilla de verificación está seleccionada, la aplicación usa datos recibidos de los servicios KSN para asegurar un tiempo de respuesta más rápido de la aplicación a nuevas amenazas y reducir la posibilidad de falsos positivos.

Si la casilla de verificación está desactivada, la tarea Análisis a pedido no usa los servicios KSN.

De forma predeterminada, la casilla está activada.

- Para asignar la prioridad base *Bajo* al proceso de trabajo en que se ejecutará la tarea, seleccione la casilla de verificación **Ejecutar tarea en segundo plano** en la ventana **Opciones**.

  La casilla de verificación modifica la prioridad de la tarea.

  Si la casilla está activada, se reduce la prioridad de la tarea en el sistema operativo. El sistema operativo proporciona recursos para realizar la tarea según la carga en la CPU y el sistema de archivos del equipo de otras aplicaciones y tareas de Kaspersky Embedded Systems Security. Como resultado, el rendimiento de las tareas se ralentizará durante el aumento de las cargas y aumentará la velocidad con cargas menores.

  Si la casilla de verificación está desactivada, la tarea se iniciará y se ejecutará con la misma prioridad que las demás aplicaciones y tareas de Kaspersky Embedded Systems Security. En este caso, aumenta la velocidad de ejecución de la tarea.

  De forma predeterminada, la casilla está desactivada.

  De manera predeterminada, a los procesos de trabajo en que se ejecutan las tareas de Kaspersky Embedded Systems Security se les asigna la prioridad *Medio* (Normal).

- Para utilizar la tarea creada como una tarea del Análisis de áreas críticas, seleccione la casilla de verificación **Considerar la tarea como análisis de áreas críticas** en la ventana **Opciones**.

  La casilla de verificación cambia la prioridad de la tarea: habilita o deshabilita el registro del evento *Análisis de áreas críticas* y la actualización del estado de protección del equipo. Kaspersky Security Center evalúa la calificación de seguridad del equipo (o los equipos) según los resultados de rendimiento de las tareas con el estado *Análisis de áreas críticas*. La casilla de verificación no está disponible en las propiedades del sistema local y las tareas personalizadas de Kaspersky Embedded Systems Security. Solo puede modificar esta configuración en Kaspersky Security Center.

  Si esta casilla de verificación está seleccionada, el Servidor de administración registra la finalización del Análisis de áreas críticas y actualiza el estado de protección del equipo según los resultados de la ejecución de la tarea. La tarea de análisis tiene una prioridad alta.

  Si la casilla de verificación está desactivada, la tarea se ejecuta con prioridad baja.

  La casilla de verificación se desactiva de forma predeterminada para tareas a pedido personalizadas.

6. Haga clic en **Siguiente**.
7. En la ventana **Programación**, configure los ajustes del inicio de la tarea programada.
8. Haga clic en **Siguiente**.
9. En la ventana **Seleccionar una cuenta para ejecutar la tarea**, especifique la cuenta que desea utilizar.
10. Haga clic en **Siguiente**.
11. Defina el nombre de la tarea.
12. Haga clic en **Siguiente**.

> El nombre de la tarea no debe tener más de 100 caracteres y no puede contener los siguientes símbolos:
> " * < > & \ : |

Se abre la ventana **Finalizar creación de la tarea**.

13. Puede ejecutar la tarea opcionalmente después de que el Asistente finalice, seleccionando la casilla **Ejecutar tarea después de que finalice el asistente**.
14. Haga clic en **Finalizar** para terminar de crear la tarea.

Se creará la nueva tarea Análisis a pedido para el equipo o el grupo de equipos seleccionado.

En esta sección

Asignar el estado de la tarea de Análisis de áreas críticas a una tarea de Análisis a pedido

De manera predeterminada, Kaspersky Security Center asigna el estado *Advertencia* al equipo si la tarea de Análisis de áreas críticas se ejecuta con menor frecuencia que la especificada por la configuración de los umbrales de generación de eventos *Hace mucho tiempo que no se realiza un análisis de áreas críticas* de Kaspersky Embedded Systems Security.

► *Para configurar el análisis de todos los equipos en un único grupo de administración, siga estos pasos:*

1. Crear una tarea de grupo de Análisis a pedido (consulte la sección “Creación de la tarea Análisis a pedido” en la página 409).
2. En la ventana **Opciones** del asistente de tareas, seleccione la casilla de verificación **Considerar la tarea como análisis de áreas críticas**. La configuración de tarea especificada (configuración de seguridad y área del análisis) se aplicará a todos los equipos del grupo. Configure la programación de la tarea.

   > Puede seleccionar la casilla de verificación **Considerar la tarea como análisis de áreas críticas** cuando crea la tarea de Análisis a pedido para un grupo de equipos o en otro momento, desde la ventana **Propiedades: <Nombre de la tarea>** (consulta la sección "Cómo abrir las propiedades de la tarea Análisis a pedido" en la página 409).

3. La utilización de una directiva nueva o existente deshabilita el inicio programado de las tareas de análisis a pedido del sistema (consulte la sección “Configuración del inicio programado de las tareas locales del sistema” en la página 96) en los equipos del grupo.

El servidor de administración de Kaspersky Security Center evaluará el estado de seguridad del equipo protegido y se lo notificará según los resultados de la última ejecución de la tarea con el estado de *Análisis de áreas críticas* y no según los resultados de la tarea del sistema de Análisis de áreas críticas.

Puede asignar el estado de la tarea de *Análisis de áreas críticas* tanto a tareas en grupo de Análisis a pedido como a tareas para conjuntos de equipos.

La Consola de la aplicación se puede utilizar para ver si la tarea de Análisis a pedido es una tarea de Análisis de áreas críticas.

En la Consola de la aplicación, la casilla de verificación **Considerar la tarea como análisis de áreas críticas** se muestra en las propiedades de la tarea, pero no se puede modificar.

Ejecución en segundo plano de una tarea de Análisis a pedido

De manera predeterminada, a los procesos en que se ejecutan las tareas de Kaspersky Embedded Systems Security se les asigna la prioridad *Medio* (Normal).

Al proceso que ejecutará una tarea de Análisis a pedido se le puede asignar la prioridad *Bajo*. Si se degrada la prioridad del proceso, se aumenta el tiempo requerido para ejecutar la tarea, pero puede tener un efecto beneficioso en la velocidad de ejecución de los procesos de otros programas activos.

Varias tareas en segundo plano pueden estar en ejecución en un único proceso de trabajo con prioridad baja. Puede especificar la cantidad máxima de procesos para las tareas de Análisis a pedido en segundo plano.

► *Para cambiar la prioridad de una tarea de Análisis a pedido existente:*

1. Abra la ventana **Propiedades: Análisis a pedido** (consulte la sección “Cómo abrir el asistente de la tarea Análisis a pedido” en la página 408).
2. Seleccione o desactive la casilla de verificación **Ejecutar tarea en segundo plano**.

   La casilla de verificación modifica la prioridad de la tarea.

   Si la casilla está activada, se reduce la prioridad de la tarea en el sistema operativo. El sistema operativo proporciona recursos para realizar la tarea según la carga en la CPU y el sistema de archivos del equipo de otras aplicaciones y tareas de Kaspersky Embedded Systems Security. Como resultado, el rendimiento de las tareas se ralentizará durante el aumento de las cargas y aumentará la velocidad con cargas menores.

   Si la casilla de verificación está desactivada, la tarea se iniciará y se ejecutará con la misma prioridad que las demás aplicaciones y tareas de Kaspersky Embedded Systems Security. En este caso, aumenta la velocidad de ejecución de la tarea.

   De forma predeterminada, la casilla está desactivada.
3. Haga clic en **Aceptar**.

La configuración de la tarea se guarda y se aplica inmediatamente a la tarea en ejecución. Si la tarea no se está ejecutando, la configuración modificada se aplica en el siguiente inicio.

Registro de la ejecución del Análisis de áreas críticas

De forma predeterminada, el estado de protección del equipo se muestra en el panel de detalles del nodo **Kaspersky Embedded Systems Security** y se actualiza cada semana después de la realización de la tarea de Análisis de áreas críticas.

La hora de actualización del estado de protección del equipo está relacionada con la programación de la tarea a pedido en cuya configuración se selecciona la casilla de verificación **Considerar la tarea como análisis de áreas críticas**. De forma predeterminada, la casilla de verificación solo se selecciona para la tarea de Análisis de áreas críticas y no se puede modificar para esta tarea.

Puede seleccionar la tarea Análisis a pedido relacionada al estado de protección del equipo solo desde Kaspersky Security Center.

Configuración del área de análisis de la tarea

Si modifica el área del análisis en las tareas Análisis al inicio del sistema operativo y Análisis de áreas críticas, puede restaurar el área del análisis predeterminado en estas tareas si restaura Kaspersky Embedded Systems Security (**Inicio** > **Programas** > **Kaspersky Embedded Systems Security** > **Modificar o eliminar Kaspersky Embedded Systems Security**). En el asistente de instalación, seleccione **Reparar componentes instalados** y haga clic en **Siguiente**, y luego seleccione la casilla de verificación **Restaurar la configuración recomendada de la aplicación**.

► *Para configurar el área de análisis para una tarea de Análisis a pedido existente:*

1. Abra la ventana **Propiedades: Análisis a pedido** (consulte la sección “Cómo abrir las propiedades de la tarea Análisis a pedido” en la página 409).
2. Seleccione la pestaña **Área del análisis**.
3. Para incluir elementos en el área del análisis:
   a. Abra el menú contextual en el espacio vacío de la lista del área de análisis.
   b. Seleccione la opción del menú contextual **Agregar área**.
   c. En la ventana abierta **Agregar objetos al área de análisis**, seleccione un tipo de objeto que desee agregar:
      - **Área predefinida** para agregar una de las áreas predefinidas en un servidor protegido. A continuación, en la lista desplegable, seleccione un área de análisis necesaria.
      - **Disco, carpeta o ubicación de red** para incluir una unidad o carpeta particular o un objeto de red en un área del análisis. A continuación, seleccione un área necesaria con un clic en el botón **Examinar**.
      - **Archivo** para incluir un archivo particular en el área del análisis. A continuación, seleccione un área necesaria con un clic en el botón **Examinar**.

      No puede agregar un objeto al área del análisis si ya se agregó como una exclusión del área del análisis.
4. Para excluir nodos individuales del área del análisis, desactive las casillas de verificación al lado de los nombres de estos nodos o siga estos pasos:
   a. Abra el menú contextual del área de análisis haciendo clic en él con el botón derecho del mouse.
   b. En el menú contextual, seleccione la opción **Agregar exclusión**.
   c. En la ventana **Agregar exclusión**, seleccione un tipo de objeto que desee agregar como una exclusión del área del análisis siguiendo la lógica del procedimiento para agregar un objeto a un área del análisis.
5. Para modificar el área del análisis o una exclusión agregada, seleccione la opción **Editar área** en el menú contextual para el área del análisis necesario.

6. Para ocultar el área del análisis agregado anteriormente o una exclusión en la lista de recursos de archivos en red, seleccione la opción **Eliminar área** en el menú contextual para el área del análisis necesario.

   El área del análisis se excluye del área de la tarea de análisis a pedido al eliminarse de la lista de recursos de archivos en red.

7. Haga clic en el botón **Aceptar**.

Se cerrará la ventana Configuración del área de análisis. Se guardaron las opciones configuradas recientemente.

Selección de niveles de seguridad predefinidos para tareas de Análisis a pedido

Se puede aplicar uno de los tres siguientes niveles de seguridad predefinidos para un elemento seleccionado en la lista de recursos de archivos en red del equipo: **Máximo Rendimiento**, **Recomendado** y **Máxima Protección**.

► *Para seleccionar uno de los niveles de seguridad predefinidos:*

1. Abra la ventana **Propiedades:** Ventana de **Análisis a pedido** (consulte la sección "**Cómo abrir las propiedades de la tarea Análisis a pedido**" en la página 409).
2. Seleccione la pestaña **Área del análisis**.
3. En la lista del equipo, seleccione un elemento incluido en el área del análisis para configurar el nivel de seguridad predefinido.
4. Haga clic en el botón **Configurar**.

   Se abre la ventana **Configuración del análisis a pedido**.
5. En la pestaña **Nivel de seguridad**, seleccione el nivel de seguridad a aplicar.

   La ventana muestra la lista de opciones de seguridad correspondientes al nivel de seguridad seleccionado.
6. Haga clic en el botón **Aceptar**.
7. Haga clic en el botón **Aceptar** en la ventana **Propiedades: Configuración del análisis a pedido**.

   La configuración de la tarea se guarda y se aplica inmediatamente a la tarea en ejecución. Si la tarea no se está ejecutando, la configuración modificada se aplica en el siguiente inicio.

Configuración manual de las opciones de seguridad

De forma predeterminada, las tareas de Análisis a pedido usan la configuración de seguridad común para toda el área del análisis. Estos ajustes corresponden a los del nivel de seguridad predefinido **Recomendado** (consulte la sección "Niveles de seguridad predefinidos", en la página 233).

Los valores predeterminados de la configuración de seguridad se pueden modificar configurándolos como valores comunes para todo el alcance de la protección, o como valores diferentes para los diversos elementos de la lista de recursos de archivos del equipo o nodos del árbol.

► *Para configurar las opciones de seguridad manualmente:*

1. Abra la ventana **Propiedades: Análisis a pedido** (consulte la sección “Cómo abrir las propiedades de la tarea Análisis a pedido” en la página 409).
2. Seleccione la pestaña **Área del análisis**.
3. Seleccione los elementos en la lista del área de análisis para la cual desea ajustar la configuración de la seguridad.

   Puede aplicarse una plantilla predefinida que contiene una configuración de seguridad (consulte la sección “Acerca de las plantillas de configuración de seguridad” en la página 155) para un nodo o elemento seleccionado en el área del análisis.

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

   Se abre la ventana **Configuración del análisis a pedido**.
5. Configure los valores de seguridad requeridos del nodo o elemento seleccionado de acuerdo con sus requisitos:
   - Configuración **General** (consulte la sección “Configuración general de las opciones de tareas”, en la página 416)
   - **Acciones** (consulte la sección “**Configuración de acciones**”, en la página 419)
   - **Rendimiento** (consulte la sección “**Configuración de rendimiento**”, en la página 421)
6. Haga clic en **Aceptar** en la ventana **Configuración del análisis a pedido**.
7. Haga clic en **Aceptar** en la ventana **Área del análisis**.

Se guarda la nueva configuración del área del análisis.

En esta sección

Configuración de las opciones generales de tareas

► *Para ajustar la configuración de la tarea de Análisis a pedido general:*

1. Abra la ventana **Propiedades:** Ventana de **Análisis a pedido** (consulte la sección “**Cómo abrir las propiedades de la tarea Análisis a pedido**” en la página 409).
2. Seleccione la pestaña **Área del análisis**.
3. Haga clic en el botón **Configurar**.

   Se abre la ventana **Configuración del análisis a pedido**.
4. Haga clic en el botón **Configurar**.

5. En la pestaña **General**, en la sección **Analizar objetos**, especifique los tipos de objetos que desea incluir en el área del análisis:

   - **Objetos para analizar**
     - **Todos los objetos**

       Kaspersky Embedded Systems Security analiza todos los objetos.

     - **Objetos analizados según su formato**

       Kaspersky Embedded Systems Security solo analiza los objetos infectables según el formato del archivo.

       Kaspersky Lab compila la lista de formatos. Se incluye en las bases de datos de Kaspersky Embedded Systems Security.

     - **Objetos analizados según la lista de extensiones de la base de datos antivirus**

       Kaspersky Embedded Systems Security solo analiza los objetos infectables según la extensión del archivo.

       Kaspersky Lab compila la lista de extensiones. Se incluye en las bases de datos de Kaspersky Embedded Systems Security.

     - **Objetos analizados según la lista de extensiones especificada**

       Kaspersky Embedded Systems Security analiza los archivos según su extensión. La lista de extensiones de archivos se puede personalizar manualmente en la ventana **Lista de extensiones**, que se puede abrir con un clic en el botón **Editar**.

   - **Subcarpetas**
   - **Subarchivos**
   - **Analizar sectores de inicio del disco y MBR**

     Habilita la protección de los sectores de inicio y los registros de inicio maestros.

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los sectores de inicio y los registros de inicio maestro en los discos duros y las unidades extraíbles del equipo.

     De forma predeterminada, la casilla está activada.

   - **Analizar secuencias alternativas de NTFS**

     Análisis de flujos de archivos y carpetas alternativos en las unidades del sistema de archivos NTFS.

     Si se selecciona la casilla de verificación, la aplicación analiza un objeto probablemente infectado y todos los flujos NTFS asociados con ese objeto.

     Si se cancela la selección de la casilla de verificación, la aplicación solo analiza el objeto que se detectó y se consideró como probablemente infectado.

     De forma predeterminada, la casilla está activada.

6. En la sección **Rendimiento**, seleccione o cancele la selección de la casilla de verificación **Analizar solo los archivos nuevos y modificados**.

   Esta casilla de verificación activa y desactiva el análisis y la protección de archivos que Kaspersky Embedded Systems Security reconoció como nuevos o modificados desde el último análisis.

   Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security

analiza y protege solo los archivos que reconoció como nuevos o modificados desde el último análisis.

Si se cancela la selección de la casilla de verificación, puede seleccionar si desea analizar y proteger solo archivos nuevos o todos los archivos, más allá de su estado de modificación.

De forma predeterminada, la casilla está activada para el nivel de seguridad **Máximo Rendimiento**. Si se configuran los niveles de seguridad **Máxima Protección** o **Recomendado**, la casilla de verificación se desactiva.

Para cambiar entre opciones disponibles cuando la casilla está desactivada, haga clic en el vínculo **Todos** / **Solo nuevos** para cada uno de los tipos de objeto compuestos.

7. En la sección **Análisis de objetos compuestos**, especifique los objetos compuestos que desea incluir en el área del análisis:

- **Todos/Solo nuevos archivos comprimidos**

  Análisis de archivos ZIP, CAB, RAR, ARJ y otros formatos de archivos.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los archivos comprimidos.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos comprimidos durante el análisis.

  El valor predeterminado depende del nivel de protección seleccionado.

- **Todos/Solo nuevos archivos SFX**

  Análisis de archivos autoextraíbles.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza archivos SFX.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos SFX durante el análisis.

  El valor predeterminado depende del nivel de protección seleccionado.

  Esta opción se encuentra activa cuando la casilla de verificación **Archivos comprimidos** está desactivada.

- **Todos/Solo nuevas bases de datos de correo electrónico**

  Análisis de archivos de bases de datos de correo de Microsoft Outlook y Microsoft Outlook Express.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza todos los archivos de la base de datos de correo.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos de la base de datos de correo durante el análisis.

  El valor predeterminado depende del nivel de seguridad seleccionado.

- **Todos/Solo nuevos objetos empaquetados**

  Análisis de archivos ejecutables empaquetados mediante compresores de código binario, tales como UPX o ASPack.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security

analiza los archivos ejecutables empaquetados por empaquetadores.

Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos ejecutables empaquetados por empaquetadores durante el análisis.

El valor predeterminado depende del nivel de protección seleccionado.

- **Todos/Solo nuevo correo electrónico simple**

  Análisis de archivos de formatos de correo, tales como mensajes de Microsoft Outlook y Microsoft Outlook Express.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los archivos con formato de correo.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos con formato de correo durante el análisis.

  El valor predeterminado depende del nivel de seguridad seleccionado.

- **Todos/Solo nuevos objetos OLE incorporados**

  Análisis de objetos integrados en archivos (por ejemplo, macros de Microsoft Word o archivos adjuntos del mensaje de correo electrónico).

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los objetos integrados en archivos.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los objetos integrados en archivos durante el análisis.

  El valor predeterminado depende del nivel de protección seleccionado.

8. Haga clic en **Aceptar**.

Se guardará la nueva configuración de la tarea.

Configuración de acciones

► *Para configurar acciones en objetos infectados y otros objetos detectados durante la ejecución de la tarea de Análisis a pedido:*

1. Abra la ventana **Propiedades:** Ventana de **Análisis a pedido** (consulte la sección "**Cómo abrir las propiedades de la tarea Análisis a pedido**" en la página 409).
2. Seleccione la pestaña **Área del análisis**.
3. Haga clic en el botón **Configurar**.

   Se abre la ventana **Configuración del análisis a pedido**.
4. Haga clic en el botón **Configurar**.
5. Seleccione la pestaña **Acciones**.
6. Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:

   - **Solo notificar**.

     Cuando se selecciona este modo, Kaspersky Embedded Systems Security no bloquea el acceso a los objetos infectados y a otros objetos detectados ni realiza ninguna acción relacionada con ellos. Se registra el siguiente evento en el registro de tareas: *Objeto no*

desinfectado. Motivo: No se tomó ninguna acción para neutralizar el objeto detectado debido a la configuración definida por el usuario. El evento especifica toda la información disponible sobre el objeto detectado.

El modo **Solo notificar** debe configurarse por separado para cada área de protección o análisis. Este modo no se usa de forma predeterminada en ninguno de los niveles de seguridad. Si selecciona este modo, Kaspersky Embedded Systems Security cambia automáticamente el nivel de seguridad a **Personalizado**.

- **Desinfectar**.
- **Desinfectar. Desinfectar; si falla la desinfección, eliminar**.
- **Eliminar**.
- **Realizar la acción recomendada**.

7. Seleccione la acción a realizar en los objetos probablemente infectados:
   - **Solo notificar**.

     Cuando se selecciona este modo, Kaspersky Embedded Systems Security no bloquea el acceso a los objetos infectados y a otros objetos detectados ni realiza ninguna acción relacionada con ellos. Se registra el siguiente evento en el registro de tareas: *Objeto no desinfectado. Motivo: No se tomó ninguna acción para neutralizar el objeto detectado debido a la configuración definida por el usuario.* El evento especifica toda la información disponible sobre el objeto detectado.

     El modo **Solo notificar** debe configurarse por separado para cada área de protección o análisis. Este modo no se usa de forma predeterminada en ninguno de los niveles de seguridad. Si selecciona este modo, Kaspersky Embedded Systems Security cambia automáticamente el nivel de seguridad a **Personalizado**.
   - **Poner en cuarentena**.
   - **Eliminar**.
   - **Realizar la acción recomendada**.
8. Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:
   a. Borre o seleccione la casilla de verificación **Realizar acciones según el tipo de objeto detectado**.

      Si se selecciona la casilla, puede configurar independientemente la acción principal y secundaria para cada tipo de objeto detectado haciendo clic en el botón **Configurar** ubicado junto a la casilla de verificación. En ese momento, Kaspersky Embedded Systems Security no permitirá abrir o ejecutar un objeto infectado, independientemente de su elección.

      Si la casilla de verificación no está seleccionada, Kaspersky Embedded Systems Security realiza las acciones seleccionadas en las secciones **Acción que se realizará con los objetos infectados y otros objetos** y **Acción que se realizará con los objetos probablemente infectados** para los tipos de objetos correspondientes.

      De forma predeterminada, la casilla está desactivada.

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

   c. En la ventana que se abre, seleccione la acción primaria y secundaria (en caso de que falle la primaria) para cada tipo de objeto detectado.

   d. Haga clic en **Aceptar**.
9. Seleccione la acción a realizar en objetos compuestos incurables: seleccione o borre la casilla de

verificación **Si se detecta un objeto integrado infectado, eliminar todo el archivo compuesto si la aplicación no puede modificarlo**.

Esta casilla habilita o deshabilita la eliminación forzada del archivo compuesto principal cuando se detecta un objeto secundario malicioso, probablemente infectado u otro objeto secundario integrado.

Si se selecciona la casilla de verificación y se configura la tarea para eliminar los objetos infectados y probablemente infectados. Kaspersky Embedded Systems Security elimina de manera forzada todo el objeto compuesto principal cuando se detecta un objeto malicioso u otro objeto integrado. La eliminación forzada de un archivo principal junto con todo su contenido sucede si la aplicación no puede eliminar únicamente el objeto secundario detectado (por ejemplo, si el objeto principal es inmodificable).

Si se desactiva esta casilla y la tarea se configura para eliminar objetos infectados y probablemente infectados, Kaspersky Embedded Systems Security no realiza la acción seleccionada si el objeto principal es inmodificable.

10. Haga clic en **Aceptar**.

Se guardará la nueva configuración de la tarea.

Configuración de rendimiento

► *Para configurar el rendimiento para la tarea Análisis a pedido:*

1. Abra la ventana **Propiedades:** Ventana de **Análisis a pedido (consulte la sección "Cómo abrir las propiedades de la tarea Análisis a pedido" en la página** 409**)**.
2. Seleccione la pestaña **Área del análisis**.
3. Haga clic en el botón **Configurar**.

   Se abre la ventana **Configuración del análisis a pedido**.
4. Haga clic en el botón **Configurar**.
5. Seleccione la pestaña **Rendimiento**.
6. En la sección **Exclusiones**:
   - Borre o seleccione la casilla de verificación **Excluir archivos**.

     Excluir archivos del análisis por nombre de archivo o máscara de nombre de archivo.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos especificados durante el análisis.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza todos los objetos.

     De forma predeterminada, la casilla está desactivada.
   - Borre o seleccione la casilla de verificación **No detectar**.

     Los objetos se excluyen del análisis por el nombre o la máscara del nombre del objeto detectable. La lista de nombres de objetos detectables está disponible en el sitio web de la Enciclopedia de Virus https://encyclopedia.kaspersky.com/knowledge/classification/

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos especificados detectables durante el análisis.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security

detecta todos los objetos especificados en la aplicación de forma predeterminada.

De forma predeterminada, la casilla está desactivada.

- Haga clic en el botón **Editar** en cada para parámetro agregar exclusiones.

7. En la sección **Configuración avanzada**:

- **Detener el análisis si demora más de (seg.)**

  Limita la duración del análisis de objetos. El valor predeterminado es 60 segundos.

  Si la casilla está desactivada, la duración del análisis se limita al valor especificado.

  Si la casilla está desactivada, la duración del análisis es ilimitada.

  De forma predeterminada, la casilla está activada para el nivel de seguridad **Máximo Rendimiento**.

- **Omitir objetos compuestos de más de (MB)**

  Excluye del análisis objetos más grandes que el tamaño especificado.

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos compuestos cuyo tamaño supera el límite especificado durante el análisis antivirus.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza los objetos compuestos de cualquier tamaño.

  De forma predeterminada, la casilla está activada para el nivel de seguridad **Máximo Rendimiento**.

- **Usar la tecnología iSwift**

  iSwift compara el identificador NTFS del archivo, que está almacenado en una base de datos, con un identificador actual. El análisis se realiza solo para archivos cuyos identificadores han cambiado (archivos nuevos y archivos modificados desde el último análisis de objetos del sistema NTFS).

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security solo analiza los archivos nuevos o modificados desde el último análisis de objetos del sistema NTFS.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza los objetos del sistema del archivo NTFS sin considerar la fecha de creación o modificación del archivo, excepto los archivos de carpetas de red.

  De forma predeterminada, la casilla está activada.

- **Usar la tecnología iChecker**

  iChecker calcula y recuerda las sumas de control de los archivos analizados. Si un objeto se modifica, la suma de control cambia. La aplicación compara todas las sumas de control durante la tarea de análisis, y analiza solo los archivos nuevos y modificados desde el último análisis.

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza solo los archivos nuevos y modificados.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza los archivos sin considerar la fecha de creación o modificación del archivo.

  De forma predeterminada, la casilla está activada.

8. Haga clic en **Aceptar**.

Se guardará la nueva configuración de la tarea.

Configuración del Análisis de unidades extraíbles

► *Para configurar el análisis de unidades extraíbles después de conectar al equipo protegido:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas.**
4. Haga doble clic en el nombre de la directiva que desea configurar.

   En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Adicional**.
5. Haga clic en el botón **Configurar** en la subsección **Análisis de unidades extraíbles**.

   Se abre la ventana **Análisis de unidades extraíbles**.
6. En la sección **Analizar al conectar**, realice las siguientes acciones:
   - Seleccione la casilla de verificación **Analizar discos extraíbles al conectarlos via USB** si desea que Kaspersky Embedded Systems Security analice automáticamente las unidades extraíbles cuando se conecten.
   - De ser necesario, seleccione **Analizar las unidades extraíbles si el volumen de los datos almacenados no excede (MB)** y especifique el valor máximo en el campo de la derecha.
   - En la lista desplegable **Analizar con nivel de seguridad**, especifique el nivel de seguridad con la configuración necesaria para el análisis de unidades extraíbles.
7. Haga clic en **Aceptar**.

La configuración especificada se guarda y se aplica.

Gestión de tareas de Análisis a pedido a través de la Consola de la aplicación

En esta sección, aprenda a navegar la interfaz de la Consola de la aplicación y establecer la configuración de la tarea en un equipo local.

En esta sección

Navegación

Sepa cómo navegar a la configuración de la tarea requerida a través de la interfaz.

En esta sección

Cómo abrir la configuración de la tarea de Análisis a pedido

► *Para abrir la configuración general de la tarea de Análisis a pedido a través de la Consola de la aplicación:*

1. Expanda el nodo **Análisis a pedido** en el árbol de la Consola de la aplicación.
2. Seleccione el nodo secundario que corresponde a la tarea que desea configurar.
3. En el nodo secundario del panel de detalles, haga clic en el vínculo **Propiedades**.

   Se abre la ventana **Configuración de tareas**.

► *Para abrir la configuración del área del análisis a través de la Consola de la aplicación:*

1. Expanda el nodo **Análisis a pedido** en el árbol de la Consola de la aplicación.
2. Seleccione el nodo secundario correspondiente a una tarea de Análisis a pedido que desea configurar.
3. En el panel de detalles del nodo seleccionado, haga clic en el vínculo **Configurar el área de análisis**.

   Se abre la ventana **Configuración del área de análisis**.

Creación y configuración de una tarea de Análisis a pedido

Las tareas personalizadas para un solo equipo pueden generarse en el nodo **Análisis a pedido**. En los otros componentes funcionales de Kaspersky Embedded Systems Security, no está disponible la creación de tareas

personalizadas.

► *Para crear y configurar una tarea nueva de Análisis a pedido:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Análisis a pedido**.
2. Seleccione **Agregar tarea**.

   Se abre la ventana **Agregar tarea**.
3. Defina los siguientes valores de configuración de tarea:
   - **Nombre**: el nombre de la tarea no puede superar los 100 caracteres y puede contener cualquier símbolo además de **" * < > & \ : |**.

     No puede guardar una tarea o configurar una tarea nueva en las pestañas **Programación**, **Avanzado** y **Ejecutar como** si el nombre de la tarea no se especifica.
   - **Descripción**: cualquier información adicional sobre la tarea, que no supere los 2000 caracteres. Esta información se mostrará en la ventana de propiedades de la tarea.
   - **Usar el analizador heurístico**.

     Esta casilla de verificación habilita y deshabilita el Analizador heurístico durante el análisis de objetos.

     Si la casilla está activada, el Analizador heurístico está habilitado.

     Si la casilla está desactivada, el Analizador heurístico está deshabilitado.

     De forma predeterminada, la casilla está activada.
   - **Ejecutar tarea en segundo plano**.

     La casilla de verificación modifica la prioridad de la tarea.

     Si la casilla está activada, se reduce la prioridad de la tarea en el sistema operativo. El sistema operativo proporciona recursos para realizar la tarea según la carga en la CPU y el sistema de archivos del equipo de otras aplicaciones y tareas de Kaspersky Embedded Systems Security. Como resultado, el rendimiento de las tareas se ralentizará durante el aumento de las cargas y aumentará la velocidad con cargas menores.

     Si la casilla de verificación está desactivada, la tarea se iniciará y se ejecutará con la misma prioridad que las demás aplicaciones y tareas de Kaspersky Embedded Systems Security. En este caso, aumenta la velocidad de ejecución de la tarea.

     De forma predeterminada, la casilla está desactivada.
   - **Aplicar la Zona de confianza**.

     Esta casilla de verificación habilita y deshabilita el uso de la Zona de confianza para una tarea.

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security agrega operaciones del archivo de procesos de confianza a las exclusiones de análisis configuradas en la tarea.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security ignora las operaciones del archivo de procesos de confianza al formar el alcance de la protección para la tarea.

De forma predeterminada, la casilla está activada.

- **Considerar la tarea como análisis de áreas críticas**.

  La casilla de verificación cambia la prioridad de la tarea: habilita o deshabilita el registro del evento *Análisis de áreas críticas* y la actualización del estado de protección del equipo. Kaspersky Security Center evalúa la calificación de seguridad del equipo (o los equipos) según los resultados de rendimiento de las tareas con el estado *Análisis de áreas críticas*. La casilla de verificación no está disponible en las propiedades del sistema local y las tareas personalizadas de Kaspersky Embedded Systems Security. Solo puede modificar esta configuración en Kaspersky Security Center.

  Si esta casilla de verificación está seleccionada, el Servidor de administración registra la finalización del Análisis de áreas críticas y actualiza el estado de protección del equipo según los resultados de la ejecución de la tarea. La tarea de análisis tiene una prioridad alta.

  Si la casilla de verificación está desactivada, la tarea se ejecuta con prioridad baja.

  La casilla de verificación se desactiva de forma predeterminada para tareas a pedido personalizadas.

- **Usar KSN para análisis**.

  Esta casilla de verificación habilita y deshabilita el uso de servicios en la nube de Kaspersky Security Network (KSN) en la tarea.

  Si la casilla de verificación está seleccionada, la aplicación usa datos recibidos de los servicios KSN para asegurar un tiempo de respuesta más rápido de la aplicación a nuevas amenazas y reducir la posibilidad de falsos positivos.

  Si la casilla de verificación está desactivada, la tarea Análisis a pedido no usa los servicios KSN.

  De forma predeterminada, la casilla está activada.

4. Configure la programación de inicio de tareas (consulte la sección "Configuración de las opciones de programación de inicio de tareas" en la página 149) en las pestañas **Programación**y **Avanzado**.
5. En la pestaña **Ejecutar como**, configure las opciones de inicio de tareas con los permisos de la cuenta (consulte la sección "Especificación de una cuenta de usuario para iniciar una tarea" en la página 151).
6. Haga clic en **Aceptar** en la ventana **Agregar tarea**.

   Se crea una nueva tarea de Análisis a pedido personalizada. Se muestra un nodo con el nombre de la tarea nueva en el árbol de la Consola de la aplicación. La operación se registra en el registro de auditoría del sistema (en la página 198).
7. Si es necesario, en el panel de detalles del nodo seleccionado, seleccione **Configurar el área de análisis**.

   Se abre la ventana **Configuración del área de análisis**.
8. En el árbol o lista de recursos del archivo del equipo, seleccione los nodos o elementos que desea incluir en el área del análisis.
9. Seleccione uno de los niveles de seguridad predefinidos (consulte la sección “Acerca de los niveles de seguridad predefinidos para tareas de Análisis a pedido” en la página 402) o configure las opciones de análisis de forma manual (consulte la sección “Configuración manual de las opciones de seguridad” en la página 431).
10. Haga clic en **Guardar** en la ventana **Configuración del área de análisis**.

Las opciones configuradas se aplican en el siguiente inicio de la tarea.

Área del análisis en tareas de Análisis a pedido

Esta sección contiene información sobre la creación y la utilización de un área del análisis en tareas del Análisis a pedido.

En esta sección

Configuración del modo de visualización para recursos de archivos en red

► *Para seleccionar un modo de visualización para los recursos de archivos en red durante la configuración del área del análisis:*

1. Abra la ventana **Configuración del área de análisis** (en la página 424).
2. Abra la lista desplegable en la sección superior izquierda de la ventana. Realice uno de los siguientes pasos:
   - Seleccione la opción **Vista de árbol** para ver los recursos de archivos en red en un modo de vista de árbol.
   - Seleccione la opción **Vista de lista** para ver los recursos de archivos en red en un modo de vista de lista.

   De forma predeterminada, los recursos de archivos en red del equipo protegido se muestran en un modo de vista de lista.
3. Haga clic en el botón **Guardar**.

Se cerrará la ventana Configuración del área de análisis. Se aplicará la configuración reciente.

Creación del área del análisis

Si administra Kaspersky Embedded Systems Security remotamente en el equipo protegido mediante la Consola de la aplicación instalada en la estación de trabajo del administrador, debe ser miembro del grupo de administradores del equipo protegido para poder ver las carpetas contenidas en él.

Los nombres de configuración pueden variar en los diferentes sistemas operativos Windows.

Si modifica el área del análisis en las tareas Análisis al inicio del sistema operativo y Análisis de áreas críticas, puede restaurar el área del análisis predeterminado en estas tareas si restaura Kaspersky Embedded Systems Security (**Inicio** > **Programas** > **Kaspersky Embedded Systems Security** > **Modificar o eliminar Kaspersky Embedded Systems Security**). En el asistente de instalación, seleccione **Reparar componentes instalados** y

haga clic en **Siguiente**, y luego seleccione la casilla de verificación **Restaurar la configuración recomendada de la aplicación**.

El procedimiento para crear el área de la tarea de Análisis a pedido depende del modo de visualización de los recursos de archivos en red (consulte la sección "Configuración del modo de visualización para recursos de archivos en red" en la página 427). Puede configurar el modo de visualización de los recursos de archivos en red como un árbol o como una lista (configurado de manera predeterminada).

► *Para crear un área del análisis con el árbol de recursos de archivos en red:*

1. Abra la ventana **Configuración del área de análisis** (en la página 424).
2. En la sección izquierda de la ventana, abra el árbol de recursos de archivos en red para ver todos los nodos y nodos secundarios.
3. Haga lo siguiente:
   - Para excluir nodos individuales del área del análisis, desactive las casillas de verificación al lado de los nombres de estos nodos.
   - Para incluir nodos individuales al área del análisis, desactive la casilla de verificación **Mi equipo** y realice lo siguiente:
     - Si desea incluir todas las unidades de un tipo en el área del análisis, seleccione la casilla opuesta al nombre del tipo de unidad requerida (por ejemplo, para agregar todas las unidades extraíbles del equipo, seleccione la casilla **Unidades extraíbles**).
     - Si desea incluir una unidad individual de un determinado tipo en el área del análisis, expanda el nodo que contiene la lista de unidades de este tipo y seleccione la casilla junto al nombre de la unidad requerida. Por ejemplo, para seleccionar la unidad extraíble **F:**, expanda el nodo **Unidades extraíbles** y seleccione la casilla de verificación para la unidad **F:**.
     - Si desea incluir solamente una carpeta o un archivo de la unidad, seleccione la casilla de verificación ubicada al lado del nombre de esa carpeta o de ese archivo.
4. Haga clic en el botón **Guardar**.

Se cerrará la ventana Configuración del área de análisis. Se guardarán las opciones configuradas recientemente.

► *Para crear un área del análisis utilizando la lista de recursos de archivos en red:*

1. Abra la ventana **Configuración del área de análisis** (en la página 424).
2. Para incluir nodos individuales al área del análisis, desactive la casilla de verificación **Mi equipo** y realice lo siguiente:
   a. Abra el menú contextual del área de análisis haciendo clic en él con el botón derecho del mouse.
   b. En el menú contextual del botón, seleccione **Agregar área de análisis**.
   c. En la ventana **Agregar área de análisis** abierta, seleccione un tipo de objeto que desee agregar:
      - **Área predefinida** para agregar una de las áreas predefinidas en un equipo protegido. A continuación, en la lista desplegable, seleccione un área de análisis necesaria.
      - **Disco, carpeta o ubicación de red** para incluir una unidad o carpeta particular o un objeto de red en un área del análisis. A continuación, seleccione un área necesaria con un clic en el botón **Examinar**.
      - **Archivo** para incluir un archivo particular en el área del análisis. A continuación, seleccione un

área necesaria con un clic en el botón **Examinar**.

No puede agregar un objeto al área del análisis si ya se agregó como una exclusión del área del análisis.

3. Para excluir nodos individuales del área del análisis, desactive las casillas de verificación al lado de los nombres de estos nodos o siga estos pasos:
   a. Abra el menú contextual del área de análisis haciendo clic en él con el botón derecho del mouse.
   b. En el menú contextual, seleccione la opción **Agregar exclusión**.
   c. En la ventana **Agregar exclusión**, seleccione un tipo de objeto que desee agregar como una exclusión del área del análisis siguiendo la lógica del procedimiento para agregar un objeto a un área del análisis.
4. Para modificar el área del análisis o una exclusión agregada, seleccione la opción **Editar área** en el menú contextual para el área del análisis necesario.
5. Para ocultar el área del análisis agregado anteriormente o una exclusión en la lista de recursos de archivos en red, seleccione la opción **Eliminar de la lista** en el menú contextual para el área del análisis necesario.

   El área del análisis se excluye del área de la tarea de Análisis a pedido al eliminarse de la lista de recursos de archivos en red.

6. Haga clic en el botón **Guardar**.

Se cerrará la ventana Configuración del área de análisis. Se guardarán las opciones configuradas recientemente.

Inclusión de objetos de red en el área del análisis

Se pueden agregar unidades, carpetas o archivos de red en el área del análisis mediante la especificación de su ruta en formato UNC (convención de nomenclatura universal).

Puede analizar carpetas de la red con la cuenta de sistema.

► *Para agregar un sitio de la red al área del análisis:*

1. Abra la ventana **Configuración del área de análisis** (en la página 424).
2. Abra la lista desplegable en la ventana del sector izquierdo superior y seleccione **Vista de árbol**.
3. En el menú contextual del nodo **Red**:
   - Seleccione **Agregar carpeta de red** si desea agregar una carpeta de red al área del análisis.
   - Seleccione **Agregar archivo de red** si desea agregar un archivo de red al área del análisis.
4. Introduzca la ruta del archivo o la carpeta de red en formato UNC y presione la tecla **INTRO**.
5. Seleccione la casilla de verificación junto al objeto de red agregado recientemente para incluirlo en el área del análisis.

6. Si es necesario, cambie la configuración de seguridad para el objeto de red agregado.
7. Haga clic en el botón **Guardar**.

Se guarda la configuración de la tarea modificada.

Creación de un área del análisis virtual

Puede incluir unidades, carpetas y archivos dinámicos en el área del análisis a fin de crear un área del análisis virtual.

> Se puede ampliar el área del análisis o protección si se agregan unidades virtuales, carpetas o archivos individuales solo si el área del análisis o protección se presenta como un árbol de recursos de archivo (consulte la sección “Configuración del modo de visualización para recursos de archivos en red”, en la página 427).

► *Para agregar una unidad virtual al área del análisis:*

1. Abra la ventana **Configuración del área de análisis** (en la página 424).
2. Abra la lista desplegable en la ventana del sector izquierdo superior y seleccione **Vista de árbol**.
3. En el árbol de recursos de archivos del equipo, abra el menú contextual en el nodo **Unidades virtuales**, haga clic en **Agregar unidad virtual** y seleccione el nombre de la unidad virtual de la lista de nombres disponibles.
4. Seleccione la casilla de verificación junto a la unidad agregada para incluirla en el área del análisis.
5. Haga clic en el botón **Guardar**.

Se guarda la configuración de la tarea modificada.

► *Para agregar un archivo o carpeta virtual al área del análisis:*

1. Abra la ventana **Configuración del área de análisis** (en la página 424).
2. Abra la lista desplegable en la ventana del sector izquierdo superior y seleccione **Vista de árbol**.
3. En el árbol de recursos de archivos del equipo, abra el menú contextual del nodo para agregar una carpeta o un archivo y seleccione una de las opciones siguientes:
   - **Agregar carpeta virtual** si desea agregar una carpeta virtual al área del análisis.
   - **Agregar archivo virtual** si desea agregar un archivo virtual al área del análisis.
4. En el campo de entrada, especifique el nombre de la carpeta o el archivo.
5. En la línea con el nombre de la carpeta o el archivo creados, seleccione la casilla de verificación para incluir esta carpeta o archivo en el área del análisis.
6. Haga clic en el botón **Guardar**.

Se guarda la configuración de la tarea modificada.

Selección de niveles de seguridad predefinidos para tareas de Análisis a pedido

Se puede aplicar uno de tres siguientes niveles de seguridad predefinidos para un nodo o un elemento seleccionado en el árbol o en la lista de recursos de archivos en red del equipo: **Máximo Rendimiento**, **Recomendado** y **Máxima**

Protección.

► *Para seleccionar uno de los niveles de seguridad predefinidos:*

1. Abra la ventana **Configuración del área de análisis** (en la página 424).
2. En el árbol o en la lista de recursos de archivos en red del equipo, seleccione un nodo o elemento para configurar el nivel de seguridad predefinido.
3. Asegúrese que el nodo o elemento seleccionado se incluya en el área del análisis.
4. En el sector derecho de la ventana, en la pestaña **Nivel de seguridad**, seleccione el nivel de seguridad que se aplicará.

   La ventana muestra la lista de opciones de seguridad correspondientes al nivel de seguridad seleccionado.
5. Haga clic en el botón **Guardar**.

   La configuración de la tarea se guarda y se aplica inmediatamente a la tarea en ejecución. Si la tarea no se está ejecutando, la configuración modificada se aplica en el siguiente inicio.

Configuración manual de las opciones de seguridad

De forma predeterminada, las tareas de Análisis a pedido usan la configuración de seguridad común para toda el área del análisis. Estos ajustes corresponden a los del nivel de seguridad predefinido **Recomendado** (consulte la sección “Niveles de seguridad predefinidos”, en la página 233).

Los valores predeterminados de la configuración de seguridad se pueden modificar configurándolos como valores comunes para todo el alcance de la protección, o como valores diferentes para los diversos elementos de la lista de recursos de archivos del equipo o nodos del árbol.

Al trabajar con el árbol de recursos de archivos en red, las opciones de seguridad que se configuran para el nodo principal seleccionado se aplican automáticamente a todos los nodos secundarios. La configuración de seguridad del nodo principal no se aplica a nodos secundarios que se configuran por separado.

► *Para configurar las opciones de seguridad manualmente:*

1. Abra la ventana **Configuración del área de análisis** (en la página 424).
2. En la sección de la ventana izquierda, seleccione el nodo o elemento para configurar las opciones de seguridad.

   Puede aplicarse una plantilla predefinida que contiene una configuración de seguridad (consulte la sección “Acerca de las plantillas de configuración de seguridad” en la página 155) para un nodo o elemento seleccionado en el área del análisis.
3. Configure los valores de seguridad requeridos del nodo o elemento seleccionado de acuerdo con sus requisitos en las siguientes pestañas:
   - Configuración general (consulte la sección “Configuración general de las opciones de tareas”, en la página 432)
   - Acciones (consulte la sección “Configuración de acciones”, en la página 434)
   - Rendimiento (consulte la sección “Configuración de rendimiento”, en la página 436)
   - Depósito jerárquico
4. Haga clic en **Guardar**en la ventana **Configuración del área de análisis**.

Se guarda la nueva configuración del área del análisis.

En esta sección

Configuración de las opciones generales de tareas

► *Para configurar las opciones de seguridad generales de la tarea de Análisis a pedido:*

1. Abra la ventana **Configuración del área de análisis** (en la página 424).
2. Seleccione la pestaña **General**.
3. En la sección **Analizar objetos**, especifique los tipos de objetos que desea incluir en el área del análisis:
   - **Objetos para analizar**
     - **Todos los objetos**

       Kaspersky Embedded Systems Security analiza todos los objetos.
     - **Objetos analizados según su formato**

       Kaspersky Embedded Systems Security solo analiza los objetos infectables según el formato del archivo.

       Kaspersky Lab compila la lista de formatos. Se incluye en las bases de datos de Kaspersky Embedded Systems Security.
     - **Objetos analizados según la lista de extensiones de la base de datos antivirus**

       Kaspersky Embedded Systems Security solo analiza los objetos infectables según la extensión del archivo.

       Kaspersky Lab compila la lista de extensiones. Se incluye en las bases de datos de Kaspersky Embedded Systems Security.
     - **Objetos analizados según la lista de extensiones especificada**

       Kaspersky Embedded Systems Security analiza los archivos según su extensión. La lista de extensiones de archivos se puede personalizar manualmente en la ventana **Lista de extensiones**, que se puede abrir con un clic en el botón **Editar**.
   - **Analizar sectores de inicio del disco y MBR**

     Habilita la protección de los sectores de inicio y los registros de inicio maestros.

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los sectores de inicio y los registros de inicio maestro en los discos duros y las unidades extraíbles del equipo.

     De forma predeterminada, la casilla está activada.
   - **Analizar secuencias alternativas de NTFS**

     Análisis de flujos de archivos y carpetas alternativos en las unidades del sistema de

archivos NTFS.

Si se selecciona la casilla de verificación, la aplicación analiza un objeto probablemente infectado y todos los flujos NTFS asociados con ese objeto.

Si se cancela la selección de la casilla de verificación, la aplicación solo analiza el objeto que se detectó y se consideró como probablemente infectado.

De forma predeterminada, la casilla está activada.

4. En la sección **Rendimiento**, seleccione o cancele la selección de la casilla de verificación **Analizar solo los archivos nuevos y modificados**.

   Esta casilla de verificación activa y desactiva el análisis y la protección de archivos que Kaspersky Embedded Systems Security reconoció como nuevos o modificados desde el último análisis.

   Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza y protege solo los archivos que reconoció como nuevos o modificados desde el último análisis.

   Si se cancela la selección de la casilla de verificación, puede seleccionar si desea analizar y proteger solo archivos nuevos o todos los archivos, más allá de su estado de modificación.

   De forma predeterminada, la casilla está activada para el nivel de seguridad **Máximo Rendimiento**. Si se configuran los niveles de seguridad **Máxima Protección** o **Recomendado**, la casilla de verificación se desactiva.

> Para cambiar entre opciones disponibles cuando la casilla está desactivada, haga clic en el vínculo **Todos** / **Solo nuevos** para cada uno de los tipos de objeto compuestos.

5. En la sección **Análisis de objetos compuestos**, especifique los objetos compuestos que desea incluir en el área del análisis:

   - **Todos/Solo nuevos archivos comprimidos**

     Análisis de archivos ZIP, CAB, RAR, ARJ y otros formatos de archivos.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los archivos comprimidos.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos comprimidos durante el análisis.

     El valor predeterminado depende del nivel de protección seleccionado.

   - **Todos/Solo nuevos archivos SFX**

     Análisis de archivos autoextraíbles.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza archivos SFX.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos SFX durante el análisis.

     El valor predeterminado depende del nivel de protección seleccionado.

     Esta opción se encuentra activa cuando la casilla de verificación **Archivos comprimidos** está desactivada.

- **Todos/Solo nuevas bases de datos de correo electrónico**

  Análisis de archivos de bases de datos de correo de Microsoft Outlook y Microsoft Outlook Express.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza todos los archivos de la base de datos de correo.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos de la base de datos de correo durante el análisis.

  El valor predeterminado depende del nivel de seguridad seleccionado.

- **Todos/Solo nuevos objetos empaquetados**

  Análisis de archivos ejecutables empaquetados mediante compresores de código binario, tales como UPX o ASPack.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los archivos ejecutables empaquetados por empaquetadores.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos ejecutables empaquetados por empaquetadores durante el análisis.

  El valor predeterminado depende del nivel de protección seleccionado.

- **Todos/Solo nuevo correo electrónico simple**

  Análisis de archivos de formatos de correo, tales como mensajes de Microsoft Outlook y Microsoft Outlook Express.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los archivos con formato de correo.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los archivos con formato de correo durante el análisis.

  El valor predeterminado depende del nivel de seguridad seleccionado.

- **Todos/Solo nuevos objetos OLE incorporados**

  Análisis de objetos integrados en archivos (por ejemplo, macros de Microsoft Word o archivos adjuntos del mensaje de correo electrónico).

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza los objetos integrados en archivos.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security omite los objetos integrados en archivos durante el análisis.

  El valor predeterminado depende del nivel de protección seleccionado.

6. Haga clic en **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de acciones

► *Para configurar las acciones en objetos infectados y otros objetos detectados para la tarea de Análisis a pedido:*

1. Abra la ventana **Configuración del área de análisis** (en la página 424).
2. Seleccione la pestaña **Acciones**.

3. Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:
   - **Solo notificar**.

     Cuando se selecciona este modo, Kaspersky Embedded Systems Security no bloquea el acceso a los objetos infectados y a otros objetos detectados ni realiza ninguna acción relacionada con ellos. Se registra el siguiente evento en el registro de tareas: *Objeto no desinfectado. Motivo: No se tomó ninguna acción para neutralizar el objeto detectado debido a la configuración definida por el usuario.* El evento especifica toda la información disponible sobre el objeto detectado.

     El modo **Solo notificar** debe configurarse por separado para cada área de protección o análisis. Este modo no se usa de forma predeterminada en ninguno de los niveles de seguridad. Si selecciona este modo, Kaspersky Embedded Systems Security cambia automáticamente el nivel de seguridad a **Personalizado**.
   - **Desinfectar**.
   - **Desinfectar. Desinfectar; si falla la desinfección, eliminar**.
   - **Eliminar**.
   - **Realizar la acción recomendada**.
4. Seleccione la acción a realizar en los objetos probablemente infectados:
   - **Solo notificar**.

     Cuando se selecciona este modo, Kaspersky Embedded Systems Security no bloquea el acceso a los objetos infectados y a otros objetos detectados ni realiza ninguna acción relacionada con ellos. Se registra el siguiente evento en el registro de tareas: *Objeto no desinfectado. Motivo: No se tomó ninguna acción para neutralizar el objeto detectado debido a la configuración definida por el usuario.* El evento especifica toda la información disponible sobre el objeto detectado.

     El modo **Solo notificar** debe configurarse por separado para cada área de protección o análisis. Este modo no se usa de forma predeterminada en ninguno de los niveles de seguridad. Si selecciona este modo, Kaspersky Embedded Systems Security cambia automáticamente el nivel de seguridad a **Personalizado**.
   - **Poner en cuarentena**.
   - **Eliminar**.
   - **Realizar la acción recomendada**.
5. Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:
   a. Borre o seleccione la casilla de verificación **Realizar acciones según el tipo de objeto detectado**.

      Si se selecciona la casilla, puede configurar independientemente la acción principal y secundaria para cada tipo de objeto detectado haciendo clic en el botón **Configurar** ubicado junto a la casilla de verificación. En ese momento, Kaspersky Embedded Systems Security no permitirá abrir o ejecutar un objeto infectado, independientemente de su elección.

      Si la casilla de verificación no está seleccionada, Kaspersky Embedded Systems Security realiza las acciones seleccionadas en las secciones **Acción que se realizará con los objetos infectados y otros objetos** y **Acción que se realizará con los objetos probablemente infectados** para los tipos de objetos correspondientes.

      De forma predeterminada, la casilla está desactivada.

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

c. En la ventana que se abre, seleccione la acción primaria y secundaria (en caso de que falle la primaria) para cada tipo de objeto detectado.

d. Haga clic en **Aceptar**.

6. Seleccione la acción a realizar en objetos compuestos incurables: seleccione o borre la casilla de verificación **Si se detecta un objeto integrado infectado, eliminar todo el archivo compuesto si la aplicación no puede modificarlo**.

   Esta casilla habilita o deshabilita la eliminación forzada del archivo compuesto principal cuando se detecta un objeto secundario malicioso, probablemente infectado u otro objeto secundario integrado.

   Si se selecciona la casilla de verificación y se configura la tarea para eliminar los objetos infectados y probablemente infectados. Kaspersky Embedded Systems Security elimina de manera forzada todo el objeto compuesto principal cuando se detecta un objeto malicioso u otro objeto integrado. La eliminación forzada de un archivo principal junto con todo su contenido sucede si la aplicación no puede eliminar únicamente el objeto secundario detectado (por ejemplo, si el objeto principal es inmodificable).

   Si se desactiva esta casilla y la tarea se configura para eliminar objetos infectados y probablemente infectados, Kaspersky Embedded Systems Security no realiza la acción seleccionada si el objeto principal es inmodificable.

7. Haga clic en **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de rendimiento

► *Para configurar el rendimiento para la tarea Análisis a pedido:*

1. Abra la ventana **Configuración del área de análisis** (en la página 424).
2. Seleccione la pestaña **Rendimiento**.
3. En la sección **Exclusiones**:
   - Borre o seleccione la casilla de verificación **Excluir archivos**.

     Excluir archivos del análisis por nombre de archivo o máscara de nombre de archivo.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos especificados durante el análisis.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza todos los objetos.

     De forma predeterminada, la casilla está desactivada.

   - Borre o seleccione la casilla de verificación **No detectar**.

     Los objetos se excluyen del análisis por el nombre o la máscara del nombre del objeto detectable. La lista de nombres de objetos detectables está disponible en el sitio web de la Enciclopedia de Virus https://encyclopedia.kaspersky.com/knowledge/classification/

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos especificados detectables durante el análisis.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security detecta todos los objetos especificados en la aplicación de forma predeterminada.

De forma predeterminada, la casilla está desactivada.

- Haga clic en el botón **Editar** en cada para parámetro agregar exclusiones.

4. En la sección **Configuración avanzada**:

- **Detener el análisis si demora más de (seg.)**

  Limita la duración del análisis de objetos. El valor predeterminado es 60 segundos.

  Si la casilla está desactivada, la duración del análisis se limita al valor especificado.

  Si la casilla está desactivada, la duración del análisis es ilimitada.

  De forma predeterminada, la casilla está activada para el nivel de seguridad **Máximo Rendimiento**.

- **Omitir objetos compuestos de más de (MB)**

  Excluye del análisis objetos más grandes que el tamaño especificado.

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos compuestos cuyo tamaño supera el límite especificado durante el análisis antivirus.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza los objetos compuestos de cualquier tamaño.

  De forma predeterminada, la casilla está activada para el nivel de seguridad **Máximo Rendimiento**.

- **Usar la tecnología iSwift**

  iSwift compara el identificador NTFS del archivo, que está almacenado en una base de datos, con un identificador actual. El análisis se realiza solo para archivos cuyos identificadores han cambiado (archivos nuevos y archivos modificados desde el último análisis de objetos del sistema NTFS).

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security solo analiza los archivos nuevos o modificados desde el último análisis de objetos del sistema NTFS.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza los objetos del sistema del archivo NTFS sin considerar la fecha de creación o modificación del archivo, excepto los archivos de carpetas de red.

  De forma predeterminada, la casilla está activada.

- **Usar la tecnología iChecker**

  iChecker calcula y recuerda las sumas de control de los archivos analizados. Si un objeto se modifica, la suma de control cambia. La aplicación compara todas las sumas de control durante la tarea de análisis, y analiza solo los archivos nuevos y modificados desde el último análisis.

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security analiza solo los archivos nuevos y modificados.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza los archivos sin considerar la fecha de creación o modificación del archivo.

  De forma predeterminada, la casilla está activada.

5. Haga clic en **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración del depósito jerárquico

► *Para configurar las acciones en objetos infectados y otros objetos detectados para la tarea de Análisis a pedido:*

1. Abra la ventana **Configuración del área de análisis** (en la página 424).
2. Seleccione la pestaña **Depósito jerárquico**.
3. Seleccione la acción que desea realizar en los archivos sin conexión:
   - **No analizar**.
   - **Analizar solo la parte residente del archivo**.
   - **Analizar todo el archivo**.

     Si selecciona esta acción, puede determinar las siguientes opciones:

     - Marque o desmarque la casilla de verificación **Solo si se accedió al archivo en el período especificado (días)** e indique el número de días.
     - Marque o desmarque la casilla de verificación **No copiar el archivo al disco duro local (de ser posible)**.
4. Haga clic en **Guardar**.

Se guardará la nueva configuración de la tarea.

Análisis de unidades extraíbles

► *Para configurar el análisis de unidades extraíbles después de conectar al equipo protegido en la Consola de la aplicación:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo de **Kaspersky Embedded Systems Security** y seleccione la opción **Configurar análisis de discos extraíbles**.

   Se abre la ventana **Análisis de unidades extraíbles**.
2. En la sección **Analizar al conectar**, realice las siguientes acciones:
   - Seleccione la casilla de verificación **Analizar discos extraíbles al conectarlos via USB** si desea que Kaspersky Embedded Systems Security analice automáticamente las unidades extraíbles cuando se conecten.
   - De ser necesario, seleccione **Analizar las unidades extraíbles si el volumen de los datos almacenados no excede (MB)** y especifique el valor máximo en el campo de la derecha.
   - En la lista desplegable **Analizar con nivel de seguridad**, especifique el nivel de seguridad con la configuración necesaria para el análisis de unidades extraíbles.
3. Haga clic en **Aceptar**.

La configuración especificada se guarda y se aplica.

Estadísticas de la tarea de Análisis a pedido

Mientras se ejecuta la tarea de Análisis a pedido, se puede visualizar información sobre la cantidad de objetos

procesados por Kaspersky Embedded Systems Security desde que se inició hasta el momento actual.

Esta información permanecerá disponible aún si se pausa la tarea. Puede ver las estadísticas de la tarea en el registro de tareas (consulte la sección “Visualización de estadísticas e información sobre una tarea de Kaspersky Embedded Systems Security en registros de tareas” en la página 202).

► *Para ver las estadísticas de una tarea de Análisis a pedido, siga estos pasos:*

1. Expanda el nodo **Análisis a pedido** en el árbol de la Consola de la aplicación.
2. Seleccione la tarea de Análisis a pedido cuyas estadísticas desea ver.

   Las estadísticas de la tarea se muestran en la sección **Estadísticas** del panel de detalles del nodo seleccionado.

En la tabla a continuación, se puede ver la información sobre los objetos procesados por Kaspersky Embedded Systems Security desde que se inició hasta el momento actual.

Tabla 61. Estadísticas de la tarea de Análisis a pedido

Campo	Descripción
Detectado	Número de objetos detectados por Kaspersky Embedded Systems Security. Por ejemplo, si Kaspersky Embedded Systems Security detecta un programa de malware en cinco archivos, el valor de este campo aumenta en uno.
Objetos infectados y otros objetos detectados	Número de objetos que Kaspersky Embedded Systems Security encontró y clasificó como infectados o número de archivos de software legítimo encontrados, que no se excluyeron del área de las tareas de Protección en tiempo real y del Análisis a pedido y se clasificaron como software legítimo que puede ser utilizado por intrusos para dañar el equipo o sus datos personales.
Objetos probablemente infectados detectados	Cantidad de objetos probablemente infectados encontrados por Kaspersky Embedded Systems Security.
Objetos no desinfectados	Cantidad de objetos que Kaspersky Embedded Systems Security no desinfectó debido a los siguientes motivos: • El tipo de objeto detectado no se puede desinfectar. • Se produjo un error durante la desinfección.
Objetos que no se pasaron a Cuarentena	Cantidad de objetos que Kaspersky Embedded Systems Security intentó poner en cuarentena pero no pudo, por ejemplo, debido a espacio insuficiente en el disco.
Objetos no eliminados	Cantidad de objetos que Kaspersky Embedded Systems Security intentó eliminar, pero no pudo hacerlo debido a que, por ejemplo, el acceso al objeto estaba bloqueado por otra aplicación.
Objetos no analizados	Cantidad de objetos en el alcance de la protección que Kaspersky Embedded Systems Security no pudo analizar debido a que, por ejemplo, el acceso al objeto estaba bloqueado por otra aplicación.
Objetos sin copia de seguridad	Cantidad de objetos cuyas copias Kaspersky Embedded Systems Security intentó guardar en Copia de seguridad, pero no pudo hacerlo; por ejemplo, debido a espacio insuficiente en el disco.
Errores de procesamiento	Cantidad de objetos en los que se produjo un error durante su procesamiento.
Objetos desinfectados	Número de objetos desinfectados por Kaspersky Embedded Systems Security.

Campo	Descripción
Pasados a Cuarentena	Número de objetos pasados a Cuarentena por Kaspersky Embedded Systems Security.
Objetos pasados a Copia de seguridad	Cantidad de copias de objetos que Kaspersky Embedded Systems Security guardó en Copia de seguridad.
Objetos eliminados	Número de objetos eliminados por Kaspersky Embedded Systems Security.
Objetos protegidos con contraseña	Cantidad de objetos (por ejemplo, archivos) que Kaspersky Embedded Systems Security omitió porque estaban protegidos por contraseña.
Objetos dañados	Cantidad de objetos omitidos por Kaspersky Embedded Systems Security debido a que el formato estaba dañado.
Objetos procesados	Cantidad total de objetos que procesó Kaspersky Embedded Systems Security.

También puede ver las estadísticas de la tarea de Análisis a pedido en el registro de tareas seleccionado si hace clic en el vínculo **Abrir el registro de tareas** en la sección **Administración** del panel de detalles.

Se recomienda procesar manualmente los eventos registrados en el registro de tareas en la pestaña **Eventos** después de la finalización de la tarea.

Zona de confianza

Esta sección brinda información sobre la Zona de confianza de Kaspersky Embedded Systems Security, así como instrucciones sobre cómo agregar objetos a la zona de confianza al ejecutar tareas.

En este capítulo

Acerca de la Zona de confianza

La Zona de confianza es una lista de exclusiones de la protección o del área del análisis que puede generar y aplicar a las tareas Análisis a pedido y Protección de archivos en tiempo real.

Si seleccionó las casillas de verificación **Agregar exclusiones recomendadas por Microsoft a la lista de exclusiones** y **Agregar exclusiones recomendadas por Kaspersky Lab a la lista de exclusiones** al instalar Kaspersky Embedded Systems Security, Kaspersky Embedded Systems Security agrega a la Zona de confianza los archivos recomendados por Microsoft y Kaspersky Lab para las tareas de Protección del equipo en tiempo real.

Puede crear una Zona de confianza en Kaspersky Embedded Systems Security según las reglas siguientes:

- Procesos de confianza. Los objetos a los que acceden los procesos de aplicaciones que son susceptibles a intersecciones de archivos se colocan en la Zona de confianza.
- Operaciones de copia de seguridad. Los objetos a los que acceden los sistemas para hacer copia de seguridad del disco duro en dispositivos externos se colocan en la Zona de confianza.
- Exclusiones. Los objetos especificados por su ubicación o un objeto detectado dentro de ellos se colocan en la Zona de confianza.

Puede aplicar la Zona de confianza a las tareas de Análisis a pedido personalizadas creadas recientemente y de Protección de archivos en tiempo real, y a todas las tareas de Análisis a pedido del sistema, excepto la tarea de Análisis de archivos en cuarentena.

La Zona de confianza se aplica a las tareas de Análisis a pedido y de Protección de archivos en tiempo real de forma predeterminada.

La lista de reglas para generar la Zona de confianza se puede exportar a un archivo de configuración con formato XML para luego importarla a Kaspersky Embedded Systems Security que se ejecuta en otro equipo.

Procesos de confianza

Se aplica a las tareas de Protección de archivos en tiempo real y Seguridad de tráfico.

Algunas aplicaciones del equipo pueden estar inestables si los archivos a los que acceden son interceptados por Kaspersky Embedded Systems Security. Dichas aplicaciones incluyen, por ejemplo, aplicaciones de controladores de dominio del sistema.

Para evitar la interrupción de la operación de dichas aplicaciones, se puede deshabilitar la protección de los archivos a los que acceden los procesos que se están ejecutando de dichas aplicaciones (se crea así una lista de

procesos de confianza dentro de la Zona de confianza).

Microsoft Corporation recomienda excluir algunos archivos del sistema operativo Microsoft Windows y archivos de aplicación de Microsoft de la Protección de archivos en tiempo real como programas que no se pueden infectar. Los nombres de algunos de dichos archivos figuran en el sitio web de Microsoft https://www.microsoft.com/en-us/ (código de artículo: KB822158).

Se puede habilitar o deshabilitar el uso de procesos de confianza en la Zona de confianza.

Si se modifica el archivo de proceso ejecutable, por ejemplo, si se actualiza, Kaspersky Embedded Systems Security lo excluirá de la lista de procesos de confianza.

La aplicación no utiliza el valor de la ruta de acceso al archivo en un equipo protegido para confiar en el proceso. La ruta al archivo en el equipo protegido solo se usa para buscar el archivo, calcular una suma de control y proveer al usuario la información sobre la fuente del archivo ejecutable.

Operaciones de copia de seguridad

Se aplica a las tareas de Protección del equipo en tiempo real.

Mientras se hacen copias de seguridad de los datos almacenados en discos en dispositivos externos, puede deshabilitar la protección de objetos a los que se puede acceder durante las operaciones de copia de seguridad. Kaspersky Embedded Systems Security analizará los objetos que la aplicación de copia de seguridad abre para la lectura con el atributo FILE_FLAG_BACKUP_SEMANTICS.

Exclusiones

Se aplica a las tareas de Protección de archivos en tiempo real y Análisis a pedido.

Puede seleccionar las tareas para las que desea utilizar cada exclusión agregada a la Zona de confianza. Además, puede excluir objetos de los análisis en la configuración del nivel de seguridad de cada tarea de Kaspersky Embedded Systems Security.

Puede agregar objetos a la zona de confianza por su ubicación en el equipo, por el nombre o la máscara del nombre del objeto detectado en esos objetos, o mediante el uso de ambos criterios.

Sobre la base de una exclusión, Kaspersky Embedded Systems Security puede omitir objetos en el desempeño de las tareas especificadas de acuerdo con la siguiente configuración:

- Objetos especificados detectables por nombre o máscara del nombre en las áreas especificadas del equipo.
- Todos los objetos detectables en las áreas especificadas del equipo.
- Objetos detectables especificados por nombre o máscara del nombre dentro de toda la protección o el área del análisis.

Gestión de la Zona de confianza mediante el Complemento de administración

En esta sección, sepa cómo navegar a través de la interfaz del Complemento de administración y configurar la Zona de confianza para una o para todos los equipos de la red.

En esta sección

Navegación

Sepa cómo navegar a la configuración de la tarea requerida a través de la interfaz.

En esta sección

Gestión de la aplicación a través de Kaspersky Security Center

► *Para abrir la Zona de confianza a través de la directiva de Kaspersky Security Center:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas.**
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Adicional**.
6. Haga clic en el botón **Configuración** en la subsección **Zona de confianza**.

   Se abre la ventana **Zona de confianza**.

Configure la directiva según sea necesario.

Si un equipo es administrado por una directiva activa de Kaspersky Security Center y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede editar a través de la Consola de la aplicación.

Cómo abrir la ventana de propiedades Zona de confianza

► *Para configurar la Zona de confianza en la ventana de propiedades de la Aplicación:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.

3. Seleccione la pestaña **Dispositivos**.
4. Abra la ventana **Propiedades: <Nombre del equipo>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre del equipo protegido
   - Seleccione el elemento **Propiedades** en el menú contextual del equipo protegido.

   Se abre la ventana **Propiedades:** Se abre la ventana **<Nombre del equipo>**.
5. En la sección **Aplicaciones**, seleccione **Kaspersky Embedded Systems Security**.
6. Haga clic en el botón **Propiedades**.

   Se abrirá la ventana **Configuración de Kaspersky Embedded Systems Security**.
7. Seleccione la sección **Adicional**.
8. Haga clic en el botón **Configuración** en la subsección **Zona de confianza**.

   Se abre la ventana **Zona de confianza**.

Configure la Zona de confianza según sea necesario.

Configuración las opciones de la Zona de confianza mediante el Complemento de administración

De manera predeterminada, la Zona de confianza se aplica a todas las tareas y directivas recientemente creadas.

Para establecer la configuración de la zona de confianza, haga lo siguiente:

1. Especifique que los objetos para omitir (consulte la Sección "Cómo agregar una exclusión" en la página 445) por Kaspersky Embedded Systems Security durante la ejecución de la tarea en la pestaña **Exclusiones**.
2. Especifique los procesos para omitir (consulte la Sección "Agregar procesos de confianza" en la página 446) por Kaspersky Embedded Systems Security durante la ejecución de la tarea en la pestaña **Procesos de confianza**.
3. Aplique la máscara de “no es un virus” (consulte la Sección “Aplicación de la máscara no es un virus” en la página 448).

En esta sección

Cómo agregar una exclusión

► *Para agregar una exclusión a la Zona de confianza mediante la directiva de Kaspersky Security Center:*

1. Abra la ventana **Zona de confianza (consulte la sección "Gestión de la aplicación a través de Kaspersky Security Center" en la página** 443**)**.
2. En la pestaña **Exclusiones**, especifique los objetos que debe omitir Kaspersky Embedded Systems Security durante el análisis:
   - Para crear exclusiones recomendadas, haga clic en el botón **Añadir exclusiones recomendadas**.

     Si hace clic en este botón, podrá ampliar la lista de exclusiones al agregar exclusiones recomendadas por Microsoft y exclusiones recomendadas por Kaspersky Lab.
   - Para importar exclusiones, haga clic en el botón **Importar** y, en la ventana que se abre, seleccione los archivos que Kaspersky Embedded Systems Security considerará de confianza.
   - Para especificar manualmente las condiciones en las cuales un archivo se considerará de confianza, haga clic en el botón **Agregar**.

     Se abre la ventana **Exclusión**.
3. En la sección **El objeto no se analizará si se cumplen las siguientes condiciones**, especifique los objetos que desea excluir del área del análisis/protección y los objetos que desea excluir de los objetos detectables:
   - Si desea excluir un objeto del alcance del análisis o protección:
     a. Seleccione la casilla de verificación **Objeto para analizar**.

        Agrega un archivo, carpeta, unidad o archivo de script a una exclusión.

        Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite el área, el archivo, la carpeta, la unidad o el archivo de script predefinido especificado al ejecutar el análisis con el uso del componente de Kaspersky Embedded Systems Security seleccionado en la sección **Área de aplicación de regla**.

        De forma predeterminada, la casilla está desactivada.

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

        Se abre la ventana **Seleccionar objeto**.

     c. Especifique el objeto que desea excluir del alcance del análisis.

        Puede usar los símbolos especiales ? y * al especificar los objetos.

     d. Haga clic en **Aceptar**.

     e. Seleccione la casilla de verificación **También aplicar a subcarpetas**, si desea excluir todos los archivos y carpetas secundarias del objeto especificado del alcance de la protección o del análisis.

- Si desea especificar el nombre de un objeto detectable:
  a. Seleccione la casilla de verificación **Objetos que detectar**.

     Los objetos se excluyen del análisis por el nombre o la máscara del nombre del objeto detectable. La lista de nombres de objetos detectables está disponible en el sitio web de la Enciclopedia de Virus.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos especificados detectables durante el análisis.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security detecta todos los objetos especificados en la aplicación de forma predeterminada.

     De forma predeterminada, la casilla está desactivada.

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

     La ventana **Lista de objetos que detectar** se abre.

  c. Especifique el nombre o la máscara del nombre del objeto detectable según la clasificación de la Enciclopedia de Virus.

  d. Haga clic en el botón **Agregar**.

  e. Haga clic en **Aceptar**.

4. En la sección **Área de aplicación de regla**, seleccione las casillas de verificación junto a los nombres de las tareas a las que se debe aplicar la exclusión.

   El nombre de la tarea de Kaspersky Embedded Systems Security en la cual se utiliza la regla.

5. Haga clic en **Aceptar**.

La exclusión se muestra en la lista en la pestaña **Exclusiones** de la ventana **Zona de confianza**.

Cómo agregar procesos de confianza

► *Para agregar uno o varios procesos a la lista de procesos de confianza:*

1. Abra la ventana **Zona de confianza** (consulte la Sección "Gestión de la aplicación a través de Kaspersky Security Center" en la página 443).
2. Seleccione la pestaña **Procesos de confianza**.
3. Seleccione la casilla de verificación **No analizar las operaciones de copia de seguridad de archivos** para omitir el análisis de las operaciones de lectura del archivo.

   La casilla de verificación habilita o deshabilita el análisis de operaciones de lectura de archivos si dichas operaciones son realizadas por las herramientas de copia de seguridad instaladas en el equipo.

   Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite las operaciones de lectura de archivos realizadas por las herramientas de copia de seguridad instaladas en el equipo.

   Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza las operaciones de lectura de archivos realizadas por las herramientas de copia de seguridad instaladas en el equipo.

   De forma predeterminada, la casilla está activada.

4. Seleccione la casilla de verificación **No analizar la actividad de archivos de los procesos especificados** para omitir el análisis de las operaciones del archivo para los procesos de confianza.

   La casilla de verificación habilita o deshabilita el análisis de la actividad de archivos de procesos de confianza.

   Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite las operaciones de los procesos de confianza durante el análisis.

   Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza las operaciones de archivos de procesos de confianza.

   De forma predeterminada, la casilla está desactivada.

5. Haga clic en el botón **Agregar**.
6. Desde el menú contextual del botón, seleccione una de las opciones:

   - **Varios procesos**.

     En la ventana **Adición de proceso de confianza** que se abre, configure lo siguiente:

     a. **Usar la ruta de acceso completa del proceso en el disco para que se considere de confianza**.

        Si la casilla se selecciona, Kaspersky Embedded Systems Security usará la ruta de acceso completa al archivo para determinar si el proceso es de confianza.

        Si la casilla de verificación está desactivada, la ruta al archivo no se utiliza para determinar si el proceso es de confianza.

        De forma predeterminada, la casilla está desactivada.

     b. **Usar hash de archivo de proceso para que se considere de confianza**.

        Si se selecciona la casilla de verificación, Kaspersky Embedded Systems Security usará el hash del archivo seleccionado para determinar el estado de confianza del proceso.

        Si la casilla de verificación está desactivada, el hash del archivo no se utiliza para determinar el estado de confianza del proceso.

        De forma predeterminada, la casilla está activada.

     c. Haga clic en el botón **Examinar** para agregar datos basados en procesos ejecutables.

     d. Seleccione un archivo ejecutable en la ventana que se abre.

        Solo puede agregar un archivo ejecutable a la vez. Repita los pasos c y d para agregar otros archivos ejecutables.

     e. Haga clic en el botón **Procesos** para agregar datos basados en procesos en ejecución.

     f. Seleccione los procesos en la ventana que se abre. Para seleccionar varios procesos, mantenga presionado el botón **CTRL** al realizar la selección.

     g. Haga clic en **Aceptar**.

Se requiere que la cuenta desde la que se ejecuta la tarea de Protección de archivos en tiempo real cuente con los derechos de administrador en el equipo con Kaspersky Embedded Systems Security instalado con el fin de autorizar la visualización de la lista de procesos activos. Se pueden ordenar los procesos en la lista de procesos activos por nombre de archivo, identificador del proceso (PID) o ruta de acceso al archivo ejecutable del proceso en el equipo local. Tenga en cuenta que para seleccionar los procesos en ejecución debe hacer clic en el botón **Procesos** usando solo la Consola de la aplicación en un equipo local o en la configuración de host especificada mediante Kaspersky Security Center.

- **Un proceso basado en el nombre y la ruta de acceso del archivo.**

  En la ventana **Agregar un proceso** que se abre, realice lo siguiente:

  a. Escriba una ruta de acceso al archivo ejecutable (incluido el nombre de archivo).

  b. Haga clic en **Aceptar**.

- **Un proceso basado en las propiedades del objeto.**

  En la ventana **Adición de proceso de confianza** que se abre, configure lo siguiente:

  a. Haga clic en el botón **Examinar** y seleccione un proceso.

  b. **Usar la ruta de acceso completa del proceso en el disco para que se considere de confianza**.

     Si la casilla se selecciona, Kaspersky Embedded Systems Security usará la ruta de acceso completa al archivo para determinar si el proceso es de confianza.

     Si la casilla de verificación está desactivada, la ruta al archivo no se utiliza para determinar si el proceso es de confianza.

     De forma predeterminada, la casilla está desactivada.

  c. **Usar hash de archivo de proceso para que se considere de confianza**.

     Si se selecciona la casilla de verificación, Kaspersky Embedded Systems Security usará el hash del archivo seleccionado para determinar el estado de confianza del proceso.

     Si la casilla de verificación está desactivada, el hash del archivo no se utiliza para determinar el estado de confianza del proceso.

     De forma predeterminada, la casilla está activada.

  d. Haga clic en **Aceptar**.

  Para agregar el proceso seleccionado a la lista de procesos de confianza, debe seleccionarse al menos un criterio de confianza.

7. En la ventana **Agregar procesos de confianza**, haga clic en el botón **Aceptar**.

El proceso o archivo seleccionado se agregará a la lista de procesos de confianza en la ventana **Zona de confianza**.

Aplicación de la máscara “no es un virus”

La máscara “no es un virus” permite omitir archivos de software y recursos web legítimos que pueden considerarse

dañinos durante el análisis. La máscara afecta las siguientes tareas:

- Protección de archivos en tiempo real.
- Análisis a pedido.

Si no se agrega la máscara a la lista de exclusiones, Kaspersky Embedded Systems Security aplicará las acciones especificadas en la configuración de la tarea para el software que caen en esta categoría.

► *Para aplicar la máscara “no es un virus”:*

1. Abra la ventana **Zona de confianza** (consulte la Sección "Gestión de la aplicación a través de Kaspersky Security Center" en la página 443).
2. En la pestaña **Exclusiones**, en la columna **Objetos que detectar**, desplácese en la lista y seleccione la línea con el valor **no es un virus:***, si la casilla de verificación está marcada.
3. Haga clic en **Aceptar**.

Se aplica la nueva configuración.

Administración de la Zona de confianza a través de la Consola de la aplicación

En esta sección, aprenda cómo navegar a través de la interfaz de la Consola de la aplicación y configurar la Zona de confianza en un equipo local.

En esta sección

Cómo aplicar Zona de confianza para tareas en la Consola de la aplicación

De forma predeterminada, la Zona de confianza se aplica a la tarea de Protección de archivos en tiempo real, las tareas definidas por el usuario de Análisis a pedido creadas recientemente y todas las tareas de Análisis a pedido del sistema, excepto la tarea de Análisis de archivos en cuarentena.

Después de que la Zona de confianza se habilita o deshabilita, las exclusiones especificadas se aplican o dejan de aplicarse inmediatamente a las tareas que se están ejecutando.

► *Para habilitar o deshabilitar la utilización de la Zona de confianza en las tareas de Kaspersky Embedded Systems Security:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nombre de la tarea para la cual desea configurar el uso de la Zona de confianza.
2. Seleccione **Propiedades**.

Se abre la ventana **Configuración de tareas**.

3. En la ventana que se abre, seleccione la pestaña **General** y realice una de las siguientes acciones:
   - Para aplicar la Zona de confianza en la tarea, active la casilla de verificación **Aplicar la Zona de confianza**.
   - Para deshabilitar la Zona de confianza en la tarea, desactive la casilla de verificación **Aplicar la Zona de confianza**.
4. Si desea ajustar la configuración de la Zona de confianza, haga clic en el vínculo del nombre de la casilla de verificación **Aplicar la Zona de confianza**.

   Se abre la ventana **Zona de confianza**.
5. Haga clic en **Aceptar** en la ventana **Configuración de tareas** para guardar los cambios.

Configuración de los parámetros de la Zona de confianza en la Consola de la aplicación

Para establecer la configuración de la zona de confianza, haga lo siguiente:

1. Especifique los objetos para omitir (consulte la Sección "Cómo agregar una exclusión a la Zona de confianza" en la página 450) por Kaspersky Embedded Systems Security durante la ejecución de la tarea en la pestaña **Exclusiones**.
2. Especifique los procesos para omitir (consulte la Sección "Procesos de confianza" en la página 452) por Kaspersky Embedded Systems Security durante la ejecución de la tarea en la pestaña **Procesos de confianza**.
3. Aplique la Zona de confianza para las tareas de la aplicación (consulte la Sección "Cómo aplicar la Zona de confianza para las tareas en la Consola de la aplicación" en la página 449).
4. Aplique la máscara de “no es un virus” (consulte la Sección “Aplicación de la máscara no es un virus” en la página 454).

En esta sección

Cómo agregar una exclusión a la Zona de confianza

► *Para agregar manualmente una exclusión a la Zona de confianza a través de la Consola de la aplicación:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security**.
2. Seleccione la opción **Configurar los parámetros de Zona de confianza** del menú.

   Se abre la ventana **Zona de confianza**.
3. Seleccione la pestaña **Exclusiones**.

4. Haga clic en el botón **Agregar**.

   Se abre la ventana **Exclusión**.

5. En la sección **El objeto no se analizará si se cumplen las siguientes condiciones**, especifique los objetos que desea excluir del área del análisis/protección y los objetos que desea excluir de los objetos detectables:

   - Si desea excluir un objeto del alcance del análisis o protección:

     a. Seleccione la casilla de verificación **Objeto para analizar**.

        Agrega un archivo, carpeta, unidad o archivo de script a una exclusión.

        Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite el área, el archivo, la carpeta, la unidad o el archivo de script predefinido especificado al ejecutar el análisis con el uso del componente de Kaspersky Embedded Systems Security seleccionado en la sección **Área de aplicación de regla**.

        De forma predeterminada, la casilla está desactivada.

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

        Se abre la ventana **Seleccionar objeto**.

     c. Especifique el objeto que desea excluir del alcance del análisis.

        Puede usar los símbolos especiales ? y * al especificar los objetos.

     d. Haga clic en **Aceptar**.

     e. Seleccione la casilla de verificación **También aplicar a subcarpetas**, si desea excluir todos los archivos y carpetas secundarias del objeto especificado del alcance de la protección o del análisis.

   - Si desea especificar el nombre de un objeto detectable:

     a. Seleccione la casilla de verificación **Objetos que detectar**.

        Los objetos se excluyen del análisis por el nombre o la máscara del nombre del objeto detectable. La lista de nombres de objetos detectables está disponible en el sitio web de la Enciclopedia de Virus.

        Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite los objetos especificados detectables durante el análisis.

        Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security detecta todos los objetos especificados en la aplicación de forma predeterminada.

        De forma predeterminada, la casilla está desactivada.

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

        La ventana **Lista de objetos que detectar** se abre.

     c. Especifique el nombre o la máscara del nombre del objeto detectable según la clasificación de la Enciclopedia de Virus.

     d. Haga clic en el botón **Agregar**.

     e. Haga clic en **Aceptar**.

6. En la sección **Área de aplicación de regla**, seleccione las casillas de verificación junto a los nombres de las tareas a las que se debe aplicar la exclusión.

   El nombre de la tarea de Kaspersky Embedded Systems Security en la cual se utiliza la

regla.

7. Haga clic en **Aceptar**.

La exclusión se muestra en la lista en la pestaña **Exclusiones** de la ventana **Zona de confianza**.

Procesos de confianza

Es posible agregar un proceso a la lista de procesos de confianza mediante uno de los siguientes métodos:

- Seleccionar el proceso de la lista de procesos actualmente en ejecución en el equipo protegido.
- Seleccionar el archivo ejecutable de un proceso sin tener en cuenta si el proceso está actualmente en ejecución.

Si se modificó el archivo ejecutable de un proceso, Kaspersky Embedded Systems Security excluye este proceso de la lista de procesos de confianza.

► *Para agregar uno o varios procesos a la lista de procesos de confianza:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security**.
2. Seleccione la opción **Configurar los parámetros de Zona de confianza** del menú.

   Se abre la ventana **Zona de confianza**.
3. Seleccione la pestaña **Procesos de confianza**.
4. Seleccione la casilla de verificación **No analizar las operaciones de copia de seguridad de archivos** para omitir el análisis de las operaciones de lectura del archivo.

   La casilla de verificación habilita o deshabilita el análisis de operaciones de lectura de archivos si dichas operaciones son realizadas por las herramientas de copia de seguridad instaladas en el equipo.

   Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite las operaciones de lectura de archivos realizadas por las herramientas de copia de seguridad instaladas en el equipo.

   Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza las operaciones de lectura de archivos realizadas por las herramientas de copia de seguridad instaladas en el equipo.

   De forma predeterminada, la casilla está activada.
5. Seleccione la casilla de verificación **No analizar la actividad de archivos de los procesos especificados** para omitir el análisis de las operaciones del archivo para los procesos de confianza.

   La casilla de verificación habilita o deshabilita el análisis de la actividad de archivos de procesos de confianza.

   Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security omite las operaciones de los procesos de confianza durante el análisis.

   Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security analiza las operaciones de archivos de procesos de confianza.

   De forma predeterminada, la casilla está desactivada.

6. Haga clic en el botón **Agregar**.
7. Desde el menú contextual del botón, seleccione una de las opciones:
   - **Varios procesos**.

     En la ventana **Adición de proceso de confianza** que se abre, configure lo siguiente:

     a. **Usar la ruta de acceso completa del proceso en el disco para que se considere de confianza**.

        Si la casilla se selecciona, Kaspersky Embedded Systems Security usará la ruta de acceso completa al archivo para determinar si el proceso es de confianza.

        Si la casilla de verificación está desactivada, la ruta al archivo no se utiliza para determinar si el proceso es de confianza.

        De forma predeterminada, la casilla está desactivada.

     b. **Usar hash de archivo de proceso para que se considere de confianza**.

        Si se selecciona la casilla de verificación, Kaspersky Embedded Systems Security usará el hash del archivo seleccionado para determinar el estado de confianza del proceso.

        Si la casilla de verificación está desactivada, el hash del archivo no se utiliza para determinar el estado de confianza del proceso.

        De forma predeterminada, la casilla está activada.

     c. Haga clic en el botón **Examinar** para agregar datos basados en procesos ejecutables.

     d. Seleccione un archivo ejecutable en la ventana que se abre.

        Solo puede agregar un archivo ejecutable a la vez. Repita los pasos c y d para agregar otros archivos ejecutables.

     e. Haga clic en el botón **Procesos** para agregar datos basados en procesos en ejecución.

     f. Seleccione los procesos en la ventana que se abre. Para seleccionar varios procesos, mantenga presionado el botón **CTRL** al realizar la selección.

     g. Haga clic en **Aceptar**.

        Se requiere que la cuenta desde la que se ejecuta la tarea de Protección de archivos en tiempo real cuente con los derechos de administrador en el equipo con Kaspersky Embedded Systems Security instalado con el fin de autorizar la visualización de la lista de procesos activos. Se pueden ordenar los procesos en la lista de procesos activos por nombre de archivo, identificador del proceso (PID) o ruta de acceso al archivo ejecutable del proceso en el equipo local. Tenga en cuenta que para seleccionar los procesos en ejecución debe hacer clic en el botón **Procesos** usando solo la Consola de la aplicación en un equipo local o en la configuración de host especificada mediante Kaspersky Security Center.

   - **Un proceso basado en el nombre y la ruta de acceso del archivo.**

     En la ventana **Agregar un proceso** que se abre, realice lo siguiente:

     a. Escriba una ruta de acceso al archivo ejecutable (incluido el nombre de archivo).

     b. Haga clic en **Aceptar**.

- **Un proceso basado en las propiedades del objeto.**

  En la ventana **Adición de proceso de confianza** que se abre, configure lo siguiente:

  a. Haga clic en el botón **Examinar** y seleccione un proceso.

  b. **Usar la ruta de acceso completa del proceso en el disco para que se considere de confianza**.

     Si la casilla se selecciona, Kaspersky Embedded Systems Security usará la ruta de acceso completa al archivo para determinar si el proceso es de confianza.

     Si la casilla de verificación está desactivada, la ruta al archivo no se utiliza para determinar si el proceso es de confianza.

     De forma predeterminada, la casilla está desactivada.

  c. **Usar hash de archivo de proceso para que se considere de confianza**.

     Si se selecciona la casilla de verificación, Kaspersky Embedded Systems Security usará el hash del archivo seleccionado para determinar el estado de confianza del proceso.

     Si la casilla de verificación está desactivada, el hash del archivo no se utiliza para determinar el estado de confianza del proceso.

     De forma predeterminada, la casilla está activada.

  d. Haga clic en **Aceptar**.

  Para agregar el proceso seleccionado a la lista de procesos de confianza, debe seleccionarse al menos un criterio de confianza.

8. En la ventana **Agregar procesos de confianza**, haga clic en el botón **Aceptar**.

El proceso o archivo seleccionado se agregará a la lista de procesos de confianza en la ventana **Zona de confianza**.

Aplicación de la máscara “no es un virus”

La máscara “no es un virus” permite omitir archivos de software y recursos web legítimos que pueden considerarse dañinos durante el análisis. La máscara afecta las siguientes tareas:

- Protección de archivos en tiempo real.
- Análisis a pedido.

Si no se agrega la máscara a la lista de exclusiones, Kaspersky Embedded Systems Security aplicará las acciones especificadas en la configuración de la tarea para el software o los recursos web que caen en esta categoría.

► *Para aplicar la máscara “no es un virus”:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security**.
2. Seleccione la opción **Configurar los parámetros de Zona de confianza** del menú.

   Se abre la ventana **Zona de confianza**.

3. Seleccione la pestaña **Exclusiones**.
4. Desplácese en la lista y seleccione la línea con el valor **no es un virus:***, si la casilla de verificación está desactivada.
5. Haga clic en **Aceptar**.

Se aplica la nueva configuración.

Prevención de exploits

Esta sección contiene instrucciones sobre cómo configurar las opciones de protección de la memoria de proceso.

En este capítulo

Acerca de la prevención de exploits

Kaspersky Embedded Systems Security proporciona la capacidad de proteger la memoria de proceso de exploits. Esta función se implementa en el componente Prevención de exploits. Puede cambiar el estado de actividad del componente y configurar las opciones de protección de memoria de proceso.

El componente protege la memoria de proceso contra exploits al insertar un Agente de protección externo (“Agente”) en el proceso protegido.

Un Agente de protección de proceso es un módulo de Kaspersky Embedded Systems Security cargado dinámicamente que se introduce en procesos protegidos para supervisar su integridad y reducir el riesgo de ataques de exploit.

La operación del Agente dentro del proceso protegido requiere iniciar y detener el proceso: la carga inicial del Agente en un proceso agregado a la lista de procesos protegidos solo es posible si el proceso se reinicia. Además, después de que un proceso se elimina de la lista de procesos protegidos, el Agente solo se puede descargar después de que el proceso se reinicie.

El Agente se debe detener para descargarlo de los procesos protegidos: si el componente Prevención de exploits no está instalado, la aplicación congela el entorno y fuerza la descarga del Agente de los procesos protegidos. Si durante la desinstalación del componente se inserta el Agente en alguno de los procesos protegidos, usted debe finalizar el proceso afectado. Es posible que se deba reiniciar el equipo (por ejemplo, si el proceso del sistema está protegido).

Si se detectan pruebas de un ataque de exploit en un proceso protegido, Kaspersky Embedded Systems Security realiza una de las siguientes acciones:

- Finaliza el proceso si se lleva a cabo un intento de ataque de exploit.
- Informa que el proceso se ha puesto en peligro.

Puede detener la protección del proceso con uno de los siguientes métodos:

- Desinstalación del componente.
- Eliminación del proceso de la lista de procesos protegidos y reinicio del proceso.

Servicio de Kaspersky Security Exploit Prevention

Se requiere el servicio de Kaspersky Security Exploit Prevention en el equipo protegido para que el componente Prevención de exploits sea más efectivo. Este servicio y el componente Prevención de exploits son parte de la instalación recomendada. Durante la instalación del servicio en el equipo protegido, se crea y se inicia el proceso kavfswh. Esto comunica la información sobre procesos protegidos del componente al Agente de seguridad.

Después de que el servicio de Kaspersky Security Exploit Prevention se detiene, Kaspersky Embedded Systems Security continúa protegiendo los procesos agregados a la lista de procesos protegidos, y también se carga en procesos agregados recientemente y se aplican todas las técnicas de prevención de exploits disponibles para proteger la memoria de proceso.

Si su equipo ejecuta el sistema operativo Windows 10 o posterior, la aplicación no continuará protegiendo los procesos y la memoria del proceso una vez que se haya detenido el servicio de Kaspersky Security Exploit Prevention.

Si el servicio de Kaspersky Security Exploit Prevention se detiene, la aplicación no recibirá información sobre eventos que ocurren con procesos protegidos (incluida información sobre ataques de exploits y cancelación de procesos). Además, el Agente no podrá recibir la información sobre la configuración de protección nueva y la adición de procesos nuevos a la lista de procesos protegidos.

Modo de Prevención de exploits

Puede seleccionar uno de los modos siguientes para configurar acciones para reducir los riesgos de que las vulnerabilidades sufran ataques de exploits en procesos protegidos:

- **Finalizar en caso de exploit**: aplique este modo para cancelar un proceso cuando se lleva a cabo un intento de exploit.

  Cuando se detecta un intento de realizar un ataque de exploit en una vulnerabilidad de un proceso del sistema operativo crítico protegido, Kaspersky Embedded Systems Security no cancela el proceso, independientemente del modo indicado en la configuración del componente Prevención de exploits.

- **Solo notificar**: aplique este modo para recibir la información sobre casos de exploits en procesos protegidos mediante eventos en el registro de seguridad.

  Si este modo se selecciona, Kaspersky Embedded Systems Security registra todos los intentos de realizar ataques de exploit en las vulnerabilidades al crear eventos.

Gestión de Prevención de exploits a través del Complemento de administración

En esta sección, aprenderá a navegar la interfaz del Complemento de administración y ajustar la configuración del componente para uno o todos los equipos en la red.

En esta sección

Navegación

Sepa cómo navegar a la configuración de la tarea requerida a través de la interfaz.

En esta sección

Cómo abrir la configuración de la directiva para la Prevención de exploits

► *Para abrir la configuración de Prevención de exploits a través de la directiva de Kaspersky Security Center:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Directivas.**
4. Haga doble clic en el nombre de la directiva que desea configurar.
5. En la ventana **Propiedades: <Nombre de la directiva>** que se abre, seleccione la sección **Protección del equipo en tiempo real**.
6. Haga clic en el botón **Configuración** en la subsección **Prevención de exploits**.

   Se abre la ventana **Prevención de exploits**.

Configure la Prevención de exploits como sea necesario.

Cómo abrir la ventana de propiedades Prevención de exploits

► *Par abrir la ventana **Propiedades:** ventana **<Nombre del servidor>** para la prevención de exploits:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Seleccione el grupo de administración para el cual desea configurar la tarea.
3. Seleccione la pestaña **Dispositivos**.
4. Abra la ventana **Propiedades: <Nombre del equipo>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre del equipo protegido
   - Seleccione el elemento **Propiedades** en el menú contextual del equipo protegido.

   Se abre la ventana **Propiedades:** Se abre la ventana **<Nombre del equipo>**.
5. En la sección **Aplicaciones**, seleccione **Kaspersky Embedded Systems Security**.
6. Haga clic en el botón **Propiedades**.

   Se abrirá la ventana **Configuración de Kaspersky Embedded Systems Security**.
7. Seleccione la sección **Protección del equipo en tiempo real**.
8. Haga clic en el botón **Configuración** en la subsección **Prevención de exploits**.

   Se abre la ventana **Prevención de exploits**.

Configure la Prevención de exploits como sea necesario.

Configuración de protección de memoria de proceso

► *Para configurar las opciones de protección de la memoria de procesos agregados a la lista de procesos protegidos, realice las siguientes acciones:*

1. Abra la ventana **Prevención de exploits** (consulte la sección "**Cómo abrir la configuración de la directiva para la Prevención de exploits**" en la página 458).
2. En el bloque **Modo de prevención de exploits**, configure las siguientes opciones:
   - **Prevenir exploit de procesos vulnerables**.

     Si se selecciona esta casilla, Kaspersky Embedded Systems Security reduce los riesgos de que las vulnerabilidades sufran ataques de exploit en los procesos de la lista de procesos protegidos.

     Si esta casilla se desactiva, Kaspersky Embedded Systems Security no protege los procesos del equipo de exploits.

     De forma predeterminada, la casilla está desactivada.
   - **Finalizar en caso de exploit**.

     Si este modo se selecciona, Kaspersky Embedded Systems Security cancela un proceso protegido al detectar un intento de ataque de exploit si una técnica de reducción de

impacto activa se ha aplicado al proceso.

- **Solo notificar**.

  Si este modo se selecciona, Kaspersky Embedded Systems Security informa los exploits al mostrar una ventana de terminal. El proceso puesto en peligro continúa ejecutándose.

  Si Kaspersky Embedded Systems Security detecta un ataque de exploit en un proceso crítico mientras se está ejecutando la aplicación en **Finalizar en caso de exploit**, el componente cambia de manera forzada al modo **Solo notificar**.

3. En el bloque **Acciones de prevención**, configure las siguientes opciones:

   - **Notificar sobre procesos abusados mediante Terminal Service.**

     Si esta casilla se selecciona, Kaspersky Embedded Systems Security muestra una ventana de terminal con una descripción que explica por qué la protección se activó y una indicación del proceso en el cual se detectó un intento de ataque de exploit.

     Si la casilla se desactiva, Kaspersky Embedded Systems Security muestra una ventana de terminal cuando se detectan un intento de ataque de exploit o la cancelación de un proceso en peligro. Una ventana de terminal se muestra sin tener en cuenta el estado del servicio de Kaspersky Security Exploit Prevention. De forma predeterminada, la casilla está activada.

   - **Prevenir exploit de procesos vulnerables incluso si el servicio de Kaspersky Security está deshabilitado**.

     Si esta casilla se selecciona, Kaspersky Embedded Systems Security reducirá el riesgo de ataques de exploit en vulnerabilidades en los procesos que se ya se hayan iniciado sin tener en cuenta si el Servicio de Kaspersky Security se está ejecutando. Kaspersky Embedded Systems Security no protegerá a los procesos agregados después de que el Servicio de Kaspersky Security se detenga. Después de que el servicio se inicie, la reducción de impacto de exploit se detendrá para todos los procesos.

     Si esta casilla se desactiva, Kaspersky Embedded Systems Security no protege a los procesos de exploits cuando el Servicio de Kaspersky Security se detiene.

     De forma predeterminada, la casilla está activada.

4. Haga clic en **Aceptar**.

Kaspersky Embedded Systems Security guarda y aplica las opciones de protección de memoria de proceso configuradas.

Cómo agregar un proceso para protección

El componente Prevención de exploits protege varios procesos de forma predeterminada. Para excluir los procesos del alcance de la protección, desactive las casillas correspondientes en la lista.

► *Para agregar un proceso a la lista de procesos protegidos:*

1. Abra la ventana **Prevención de exploits** (consulte la sección "**Cómo abrir la configuración de la directiva para la Prevención de exploits**" en la página 458).
2. En la pestaña **Procesos protegidos**, haga clic en el botón **Examinar**.

   Se abre la ventana del Explorador de Microsoft Windows.
3. Seleccione el proceso que desea agregar a la lista.

4. Haga clic en el botón **Abrir**.

   Se muestra el nombre de proceso en la línea.

5. Haga clic en el botón **Agregar**.

   El proceso se añadirá a la lista de procesos protegidos.

6. Seleccione el proceso agregado.
7. Haga clic en **Configurar técnicas de prevención de exploits**.

   Se abre la ventana **Técnicas de prevención de exploits**.

8. Seleccione una de las opciones para aplicar técnicas de reducción de impacto:

   - **Aplicar todas las técnicas de prevención de exploits disponibles**.

     Si se selecciona esta opción, la lista no se puede modificar. Todas las técnicas disponibles para un proceso se aplican de forma predeterminada.

   - **Aplicar las técnicas de prevención de exploits seleccionadas**.

     Si esta opción se selecciona, puede modificar la lista de técnicas de reducción de impacto aplicadas:

     a. Seleccione las casillas al lado de las técnicas que desea aplicar para proteger el proceso seleccionado.

     b. Seleccione o desactive la casilla de verificación **Aplicar técnica de Reducción de la superficie de ataque**.

9. Configure las opciones de la Técnica de reducción de la superficie de ataque:

   - Ingrese los nombres de los módulos cuyo inicio se bloqueará desde el proceso protegido en el campo **Denegar módulos**.
   - En el campo **No denegar módulos si se cargan en la zona de Internet**, seleccione las casillas al lado de las opciones en las cuales desea permitir que se inicien los módulos:
     - Internet
     - Intranet local
     - Sitios web de confianza
     - Sitios restringidos
     - Equipo

     Estas configuraciones solo se aplican a Internet Explorer®.

10. Haga clic en **Aceptar**.

El proceso se añade al alcance de la protección de la tarea.

Gestión de Prevención de exploits a través de la Consola de la aplicación

En esta sección, aprenda a navegar la interfaz de la Consola de la aplicación y establecer la configuración del componente en un equipo local.

En esta sección

Navegación

Sepa cómo navegar a la configuración de la tarea requerida a través de la interfaz.

En esta sección

Cómo abrir la configuración general de Prevención de exploits

► *Para abrir la ventana **Ajustes de prevención de exploits**:*

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security**.
2. Abra el menú contextual y seleccione la opción de menú **Prevención de exploits: ajustes generales**.

   Se abre la ventana **Ajustes de prevención de exploits**.

Ajuste la configuración general para la Prevención de exploits como sea necesario.

Cómo abrir la configuración de protección de procesos de Prevención de exploits

► *Para abrir la ventana **Ajustes de protección de los procesos**:*

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Kaspersky Embedded Systems Security**.
2. Abra el menú contextual y seleccione la opción de menú **Prevención de exploits: configuración de protección de procesos**.

   Se abre la ventana **Ajustes de protección de los procesos**.

Ajuste la configuración de protección de procesos de Prevención de exploits como sea necesario.

Configuración de protección de memoria de proceso

► *Para agregar un proceso a la lista de procesos protegidos:*

1. Abra la ventana Ajustes de prevención de exploits.
2. En el bloque **Modo de prevención de exploits**, configure las siguientes opciones:
   - **Prevenir exploit de procesos vulnerables**.

     Si se selecciona esta casilla, Kaspersky Embedded Systems Security reduce los riesgos de que las vulnerabilidades sufran ataques de exploit en los procesos de la lista de

procesos protegidos.

Si esta casilla se desactiva, Kaspersky Embedded Systems Security no protege los procesos del equipo de exploits.

De forma predeterminada, la casilla está desactivada.

- **Finalizar en caso de exploit**.

  Si este modo se selecciona, Kaspersky Embedded Systems Security cancela un proceso protegido al detectar un intento de ataque de exploit si una técnica de reducción de impacto activa se ha aplicado al proceso.

- **Solo notificar**.

  Si este modo se selecciona, Kaspersky Embedded Systems Security informa los exploits al mostrar una ventana de terminal. El proceso puesto en peligro continúa ejecutándose.

  Si Kaspersky Embedded Systems Security detecta un ataque de exploit en un proceso crítico mientras se está ejecutando la aplicación en **Finalizar en caso de exploit**, el componente cambia de manera forzada al modo **Solo notificar**.

3. En el bloque **Acciones de prevención**, configure las siguientes opciones:

   - **Notificar sobre procesos abusados mediante Terminal Service.**

     Si esta casilla se selecciona, Kaspersky Embedded Systems Security muestra una ventana de terminal con una descripción que explica por qué la protección se activó y una indicación del proceso en el cual se detectó un intento de ataque de exploit.

     Si la casilla se desactiva, Kaspersky Embedded Systems Security muestra una ventana de terminal cuando se detectan un intento de ataque de exploit o la cancelación de un proceso en peligro. Una ventana de terminal se muestra sin tener en cuenta el estado del servicio de Kaspersky Security Exploit Prevention. De forma predeterminada, la casilla está activada.

   - **Prevenir exploit de procesos vulnerables incluso si el servicio de Kaspersky Security está deshabilitado**.

     Si esta casilla se selecciona, Kaspersky Embedded Systems Security reducirá el riesgo de ataques de exploit en vulnerabilidades en los procesos que se ya se hayan iniciado sin tener en cuenta si el Servicio de Kaspersky Security se está ejecutando. Kaspersky Embedded Systems Security no protegerá a los procesos agregados después de que el Servicio de Kaspersky Security se detenga. Después de que el servicio se inicie, la reducción de impacto de exploit se detendrá para todos los procesos.

     Si esta casilla se desactiva, Kaspersky Embedded Systems Security no protege a los procesos de exploits cuando el Servicio de Kaspersky Security se detiene.

     De forma predeterminada, la casilla está activada.

4. En la ventana **Ajustes de prevención de exploits**, haga clic en **Aceptar**.

Kaspersky Embedded Systems Security guarda y aplica las opciones de protección de memoria de proceso configuradas.

Cómo agregar un proceso para protección

El componente Prevención de exploits protege varios procesos de forma predeterminada. Puede desmarcar los procesos que no desea proteger en la lista de procesos protegidos.

► *Para agregar un proceso a la lista de procesos protegidos:*

1. Abra la ventana Ajustes de protección de los procesos.

2. Para agregar un proceso para protegerlos de abuso y reducir el mayor impacto de exploit posible, realice las siguientes acciones:
   a. Haga clic en el botón **Examinar**.

      Se abre la ventana estándar **Abrir** de Microsoft Windows.

   b. En la ventana que se abre, seleccione el proceso que quiere añadir a la lista.
   c. Haga clic en el botón **Abrir**.
   d. Haga clic en el botón **Agregar**.

      El proceso se añadirá a la lista de procesos protegidos.
3. Seleccione un proceso de la lista.
4. En la configuración actual **Ajustes de protección de los procesos**, se muestra lo siguiente:
   - **Nombre del proceso**.
   - **Se está ejecutando**.
   - **Técnicas de prevención de exploits aplicadas**.
   - **Configuración de reducción de la superficie de ataque**.
5. Para modificar las técnicas de prevención de exploits que se aplican al proceso, seleccione la pestaña **Técnicas de prevención de exploits**.
6. Seleccione una de las opciones para aplicar técnicas de reducción de impacto:
   - **Aplicar todas las técnicas de prevención de exploits disponibles**.

     Si se selecciona esta opción, la lista no se puede modificar. Todas las técnicas disponibles para un proceso se aplican de forma predeterminada.
   - **Aplicar las técnicas de prevención de exploits enumeradas al proceso**.

     Si esta opción se selecciona, puede modificar la lista de técnicas de reducción de impacto aplicadas:

     a. Seleccione las casillas al lado de las técnicas que desea aplicar para proteger el proceso seleccionado.
7. Configure las opciones de la Técnica de reducción de la superficie de ataque:
   - Ingrese los nombres de los módulos cuyo inicio se bloqueará desde el proceso protegido en el campo **Denegar módulos**.
   - En el campo **No denegar módulos si se cargan en la zona de Internet**, seleccione las casillas al lado de las opciones en las cuales desea permitir que se inicien los módulos:
     - Internet
     - Intranet local
     - Sitios web de confianza
     - Sitios restringidos
     - Equipo

     Estas configuraciones solo se aplican a Internet Explorer®.
8. Haga clic en **Aceptar**.

El proceso se añade al alcance de la protección de la tarea.

Técnicas de prevención de exploits

Tabla 62. Técnicas de prevención de exploits

Técnica de prevención de exploits	Descripción
Prevención de ejecución de datos (DEP)	La prevención de ejecución de datos bloquea la ejecución del código arbitrario en áreas protegidas de la memoria.
Randomización del diseño del espacio de direcciones (ASLR)	Cambia el diseño de estructuras de datos en el espacio de direcciones del proceso.
Protección de sobrescritura del controlador de excepciones estructuradas (SEHOP)	Reemplazo de registros de excepciones o reemplazo del controlador de excepciones.
Asignación de página nula	Prevención de desvío el indicador nulo
Verificación de llamada de la red de LoadLibrary (anti-ROP)	Protección contra DLL de carga desde rutas de la red.
Pilas ejecutables (anti ROP)	Bloqueo de ejecución no autorizada de áreas de las pilas.
Verificación anti RET (anti ROP)	Compruebe que la instrucción de LLAMADA se invoque de manera segura.
Anti traslado de pilas (anti ROP)	La Protección contra el traslado de indicadores de pilas de ESP a una dirección ejecutable.
Monitor de acceso a la función exportar tabla de direcciones simple (Monitor de acceso a EAT y Monitor de acceso a EAT mediante el registro de depuraciones)	Protección de acceso de lectura a la función exportar tabla de direcciones para kernel32.dll, kernelbase.dll y ntdll.dll.
Asignación de Heap Spray (Heapspray)	Protección contra asignación de memoria para ejecutar código malicioso.
Simulación del flujo de ejecución (programación orientada a la antidevolución)	Detección de cadenas sospechosas de instrucciones (posible gadget ROP) en el componente API de Windows.
Monitor de llamada de IntervalProfiler (Protección del controlador funcional auxiliar [AFDP])	Protección contra elevación de privilegios a través de una vulnerabilidad en el controlador AFD (ejecución de código arbitrario en anillo 0 a través de una llamada de QueryIntervalProfile).
Reducción de la superficie de ataque (ASR)	Bloqueo del inicio de complementos automáticos vulnerables mediante el proceso protegido.
Hollowing antiproceso (Hollowing)	Protección contra creación y ejecución de copias maliciosas de procesos de confianza.
Anti AtomBombing (APC)	Exploit de la tabla de atom global mediante llamadas de procedimiento asíncronas (APC).
Anti CreateRemoteThread (RThreadLocal)	Otro proceso ha creado un subproceso en el proceso protegido.

Técnica de prevención de exploits	Descripción
Anti CreateRemoteThread (RThreadRemote)	El proceso protegido ha creado un subproceso en otro proceso.

Integración con sistemas de terceros

Esta sección describe la integración de Kaspersky Embedded Systems Security con funciones y tecnologías de terceros.

En este capítulo

Control del rendimiento. Contadores de Kaspersky Embedded Systems Security

Esta sección brinda información sobre los contadores de Kaspersky Embedded Systems Security: Contadores de rendimiento del Supervisor del sistema y contadores y capturas de SNMP.

En esta sección

Contadores de rendimiento para el supervisor del sistema

Esta sección contiene información sobre contadores de rendimiento para el supervisor del sistema de Microsoft Windows que Kaspersky Embedded Systems Security registra durante la instalación.

En esta sección

Acerca de los contadores de rendimiento de Kaspersky Embedded Systems Security

El componente **Contadores de rendimiento** está incluido en los componentes instalados de Kaspersky Embedded Systems Security de forma predeterminada. Kaspersky Embedded Systems Security registra sus propios contadores de rendimiento en el supervisor del sistema de Microsoft Windows durante la instalación.

Mediante contadores de Kaspersky Embedded Systems Security, puede supervisar el rendimiento de la aplicación mientras se ejecutan tareas de Protección en tiempo real. Puede descubrir lugares estrechos cuando se ejecuta con otras aplicaciones y escasez de recursos. Puede diagnosticar la configuración no deseada de Kaspersky Embedded Systems Security, así como interrupciones en su funcionamiento.

Puede ver los contadores de rendimiento de Kaspersky Embedded Systems Security si abre la consola **Rendimiento** en el elemento **Administración** del Panel de control de Windows.

Las siguientes secciones enumeran definiciones de contadores, intervalos recomendados para obtener lecturas, valores de umbral y recomendaciones para la configuración de Kaspersky Embedded Systems Security si los valores del contador los superan.

Cantidad total de solicitudes denegadas

Tabla 63. Cantidad total de solicitudes denegadas

Nombre	Cantidad total de solicitudes denegadas
Definición	Cantidad total de solicitudes del controlador de interceptación de archivos para procesar los objetos que no fueron aceptados por procesos de la aplicación, obtenida desde el último inicio de Kaspersky Embedded Systems Security. La aplicación omite objetos para los cuales las solicitudes del procesamiento son denegadas por procesos de Kaspersky Embedded Systems Security.
Objetivo	Este contador puede ayudarlo a detectar: • Protección en tiempo real de menor calidad a raíz del atascamiento de los procesos de trabajo de Kaspersky Embedded Systems Security • Interrupciones en la Protección en tiempo real debido a errores de distribuidor para la interceptación de archivos.
Valor umbral/ normal	0 / 1.
Intervalo de lectura recomendado	1 hora.
Recomendaciones para la configuración si el valor supera el umbral	La cantidad de solicitudes del proceso denegadas corresponde a la cantidad de objetos omitidos. Las siguientes situaciones son posibles según el comportamiento del contador: • El contador muestra varias solicitudes denegadas durante el período extendido: todos los procesos de Kaspersky Embedded Systems Security se cargan totalmente para que Kaspersky Embedded Systems Security no pueda analizar objetos. Para evitar que se omitan objetos, aumente el número de procesos de la aplicación para las tareas de Protección en tiempo real. Puede usar configuraciones de Kaspersky Embedded Systems Security como **Número máximo de procesos activos** y **Número de procesos para la protección en tiempo real**; • La cantidad de solicitudes denegadas supera de manera considerable el umbral crítico y aumenta rápidamente: el distribuidor para la interceptación de archivos dejó de funcionar. Kaspersky Embedded Systems Security no está analizando objetos durante el acceso. Reinicie Kaspersky Embedded Systems Security.

Cantidad total de solicitudes omitidas

Tabla 64. Cantidad total de solicitudes omitidas

Nombre	Cantidad total de solicitudes omitidas
Definición	La cantidad total de solicitudes del controlador de interceptación de archivos para procesar objetos que recibió Kaspersky Embedded Systems Security pero que no generaron eventos de finalización de procesamiento. Esta cantidad se cuenta desde el momento en que la aplicación se inició por última vez. Si una solicitud para procesar ese objeto aceptada por uno de los procesos de trabajo no envió un evento para que finalice el procesamiento, el controlador transferirá dicha solicitud a otro proceso y el valor del contador **Cantidad total de solicitudes omitidas** se incrementará en 1. Si el controlador revisó todos los procesos en ejecución y ningún proceso recibió la solicitud de procesamiento (por estar ocupados) ni envió ningún evento de finalización de proceso, Kaspersky Embedded Systems Security omitirá dicho objeto, y el valor del contador **Cantidad total de solicitudes omitidas** se incrementará en 1.
Objetivo	Este contador le permite detectar bajas en el rendimiento debido a errores del distribuidor para la interceptación de archivos.
Valor umbral/ normal	0 / 1
Intervalo de lectura recomendado	1 hora
Recomendaciones para la configuración si el valor supera el umbral	Si el valor del contador es distinto de cero, significa que uno o varios flujos del distribuidor para la interceptación de archivos está interrumpido y no funciona. El valor del contador corresponde a la cantidad de flujos actualmente inactivos. Si la velocidad del análisis no es satisfactoria, reinicie Kaspersky Embedded Systems Security a fin de restaurar los flujos fuera de línea.

Cantidad de solicitudes sin procesar por falta de recursos del sistema

Tabla 65. Cantidad de solicitudes sin procesar por falta de recursos del sistema

Nombre	Cantidad de solicitudes sin procesar por falta de recursos.
Definición	Cantidad total de solicitudes del controlador de interceptación de archivos que no se procesaron por falta de recursos del sistema (por ejemplo, de memoria RAM), calculada desde el último inicio de Kaspersky Embedded Systems Security. Kaspersky Embedded Systems Security omite las solicitudes de procesamiento de objetos que no son procesadas por el controlador de interceptación de archivos.
Objetivo	Este contador se puede usar para detectar y eliminar una posible menor calidad de la Protección en tiempo real que se produce debido a una baja de recursos del sistema.
Valor umbral/ normal	0 / 1.

Intervalo de lectura recomendado	1 hora.
Recomendaciones para la configuración si el valor supera el umbral	Si el valor del contador no es cero, los procesos en ejecución de Kaspersky Embedded Systems Security necesitan más RAM para procesar solicitudes. Es posible que los procesos activos de otras aplicaciones estén usando toda la memoria RAM disponible.

Cantidad de solicitudes enviadas para su proceso

Tabla 66. Cantidad de solicitudes enviadas para su proceso

Nombre	Cantidad de solicitudes enviadas para su proceso.
Definición	La cantidad de objetos que esperan ser procesados por los procesos de trabajo.
Objetivo	Este contador se puede usar para hacer un seguimiento de la carga de los procesos en ejecución de Kaspersky Embedded Systems Security y del nivel general de la actividad de los archivos en el equipo.
Valor umbral/ normal	El valor el contador puede variar según el nivel de la actividad de los archivos en el equipo.
Intervalo de lectura recomendado	1 minuto
Recomendaciones para la configuración si el valor supera el umbral	No

Cantidad promedio de flujos del distribuidor para la interceptación de archivos

Tabla 67. Cantidad promedio de flujos del distribuidor para la interceptación de archivos

Nombre	Cantidad promedio de flujos del distribuidor para la interceptación de archivos.
Definición	La cantidad de flujos del distribuidor para la interceptación de archivos en un proceso y el promedio de todos los procesos actualmente involucrados en tareas de Protección en tiempo real.
Objetivo	Este contador se puede usar para detectar y eliminar una posible menor calidad de la Protección en tiempo real que se produce porque los procesos de Kaspersky Embedded Systems Security se ejecutan con carga completa.
Valor umbral/ normal	Varía / 40
Intervalo de lectura recomendado	1 minuto

Recomendaciones para la configuración si el valor supera el umbral	Se pueden crear hasta 60 flujos del distribuidor para la interceptación de archivos en cada proceso de trabajo. Si el valor del contador se acerca a 60, existe el riesgo de que ninguno de los procesos en ejecución pueda procesar la solicitud siguiente en la cola del controlador de interceptación de archivos y de que Kaspersky Embedded Systems Security omita el objeto. Aumente la cantidad de procesos de Kaspersky Embedded Systems Security para las tareas de Protección en tiempo real. Puede usar dicha configuración de Kaspersky Embedded Systems Security como **Número máximo de procesos activos** y **Número de procesos para la protección en tiempo real**.

Cantidad máxima de flujos del distribuidor para la interceptación de archivos

Tabla 68. Cantidad máxima de flujos del distribuidor para la interceptación de archivos

Nombre	Cantidad máxima de flujos del distribuidor para la interceptación de archivos.
Definición	La cantidad de flujos del distribuidor para la interceptación de archivos en un proceso y la cantidad máxima de todos los procesos actualmente involucrados en tareas de Protección en tiempo real.
Objetivo	Este contador le permite detectar y eliminar bajas de rendimiento debido a una distribución de cargas dispar en los procesos en ejecución.
Valor umbral/ normal	Varía / 40
Intervalo de lectura recomendado	1 minuto
Recomendaciones para la configuración si el valor supera el umbral	Si el valor del contador supera de manera considerable y continua el valor siguiente del contador **Cantidad promedio de flujos de distribuidor para la interceptación de archivos**, Kaspersky Embedded Systems Security está distribuyendo la carga para los procesos en ejecución de manera dispar. Reinicie Kaspersky Embedded Systems Security.

Cantidad de elementos en la cola de objetos infectados

Tabla 69. Cantidad de elementos en la cola de objetos infectados

Nombre	Cantidad de elementos en la cola de objetos infectados.
Definición	Cantidad de objetos infectados que actualmente esperan ser procesados (desinfectados o eliminados).
Objetivo	Este contador puede ayudarlo a detectar: • Interrupciones en la Protección en tiempo real debido a posibles errores de distribuidor para la interceptación de archivos. • Sobrecarga de procesos debido a una distribución dispar del tiempo del procesador entre diferentes procesos en ejecución y Kaspersky Embedded Systems Security. • Ataques de virus.

Valor umbral/ normal	Este valor puede ser distinto de cero mientras Kaspersky Embedded Systems Security procesa objetos infectados o probablemente infectados, pero regresará a cero cuando el procesamiento haya finalizado./El valor se mantiene distinto de cero durante un período prolongado.
Intervalo de lectura recomendado	1 minuto
Recomendaciones para la configuración si el valor supera el umbral	Si el valor del contador no regresa a cero durante un periodo prolongado: • Kaspersky Embedded Systems Security no está procesando objetos (es posible que se haya interrumpido el distribuidor para la interceptación de archivos); Reinicie Kaspersky Embedded Systems Security. • El tiempo del procesador es insuficiente para procesar los objetos. Asegúrese de que Kaspersky Embedded Systems Security reciba tiempo adicional del procesador (por ejemplo, disminuya la carga de otras aplicaciones en el equipo). • Se produjo un brote de virus. Una gran cantidad de objetos infectados o probablemente infectados en la tarea de Protección de archivos en tiempo real también es un signo de un brote de virus. Puede consultar la información sobre el número de objetos detectados en las estadísticas de la tarea o los registros de tareas.

Cantidad de objetos procesados por segundo

Tabla 70. Cantidad de objetos procesados por segundo

Nombre	Cantidad de objetos procesados por segundo.
Definición	Cantidad de objetos procesados dividida por la cantidad de tiempo empleado para procesar esos objetos (calculada durante intervalos de tiempo idénticos).
Objetivo	Este contador refleja la velocidad de procesamiento de objetos. Se puede usar para detectar y eliminar niveles bajos de rendimiento del equipo que se producen debido a que el procesador asigna tiempo insuficiente a los procesos de Kaspersky Embedded Systems Security o debido a errores en la operación de Kaspersky Embedded Systems Security.
Valor umbral/ normal	Varía / n.º
Intervalo de lectura recomendado	1 minuto.

Recomendaciones para la configuración si el valor supera el umbral	Los valores de este contador dependen de los valores establecidos en la configuración de Kaspersky Embedded Systems Security y de la carga de procesos de otras aplicaciones en el equipo. Observe el nivel promedio de las cantidades del contador durante un periodo prolongado. Si disminuye el nivel general de los valores del contador, es posible que se haya producido una de las siguientes situaciones: • Los procesos de Kaspersky Embedded Systems Security no disponen del tiempo del procesador necesario para procesar los objetos. Asegúrese de que Kaspersky Embedded Systems Security reciba tiempo adicional del procesador (por ejemplo, disminuya la carga de otras aplicaciones en el equipo). • Kaspersky Embedded Systems Security experimentó un error (varios flujos están inactivos). Reinicie Kaspersky Embedded Systems Security.

Contadores y capturas SNMP de Kaspersky Embedded Systems Security

Esta sección contiene información sobre contadores y capturas de Kaspersky Embedded Systems Security.

En esta sección

Acerca de contadores y capturas SNMP de Kaspersky Embedded Systems Security

Si ha incluido Contadores y capturas SNMP en el conjunto de componentes Antivirus para instalar, puede ver contadores y capturas de Kaspersky Embedded Systems Security a través del Protocolo simple de administración de redes (SNMP).

Para ver los contadores y las capturas de Kaspersky Embedded Systems Security desde la estación de trabajo del administrador, inicie el servicio SNMP en el equipo protegido e inicie los servicios de capturas SNMP en la estación de trabajo del administrador.

Contadores SNMP de Kaspersky Embedded Systems Security

Esta sección contiene tablas con una descripción de la configuración para los contadores SNMP de Kaspersky Embedded Systems Security.

En esta sección

Contadores de rendimiento

Tabla 71. Contadores de rendimiento

Contador	Definición
currentRequestsAmount	Cantidad de solicitudes enviadas para su proceso (en la página 470)
currentInfectedQueueLength	Número de elementos en la cola de objetos infectados (consulte la sección “Número de elementos en la cola de objetos infectados”, en la página 471)
currentObjectProcessingRate	Cantidad de objetos procesados por segundo (en la página 472)
currentWorkProcessesNumber	Cantidad actual de procesos de trabajo utilizados por Kaspersky Embedded Systems Security

Contadores de cuarentena

Tabla 72. Contadores de cuarentena

Contador	Definición
totalObjects	Cantidad de objetos que se encuentran actualmente en cuarentena
totalSuspiciousObjects	Cantidad de objetos probablemente infectados que se encuentran actualmente en cuarentena
currentStorageSize	Tamaño total de datos en cuarentena (MB)

Contador de Copia de seguridad

Tabla 73. Contador de Copia de seguridad

Contador	Definición
currentBackupStorageSize	Tamaño total de datos en copia de seguridad (MB)

Contadores generales

Tabla 74. Contadores generales

Contador	Definición
lastCriticalAreasScanAge	El periodo desde el último análisis completo de las áreas críticas del equipo (tiempo transcurrido en segundos desde que se completó la última tarea de *Análisis de áreas críticas*).
licenseExpirationDate	Fecha de caducidad de la licencia. Si se ha agregado una clave activa y claves adicionales, se muestra la fecha de caducidad de la licencia asociada con la clave adicional.
currentApplicationUptime	Cantidad de tiempo que Kaspersky Embedded Systems Security ha estado en ejecución desde su último inicio, en centésimos de segundos.
currentFileMonitorTaskStatus	Estado de la tarea de Protección de archivos en tiempo real: **Encendido**: en ejecución; **Apagado**: detenida o en pausa.

Contador de actualización

Tabla 75. Contador de actualización

Contador	Definición
avBasesAge	"Antigüedad" de las bases de datos (tiempo transcurrido en centésimos de segundos desde la fecha de creación de las bases de datos con las últimas actualizaciones instaladas).

Contadores de protección en tiempo real

Tabla 76. Contadores de protección en tiempo real

Contador	Definición
totalObjectsProcessed	Cantidad total de objetos analizados desde la hora en que se ejecutó la última tarea de Protección de archivos en tiempo real
totalInfectedObjectsFound	Cantidad total de Objetos infectados y otros objetos detectados desde la hora en que se ejecutó la última tarea de Protección de archivos en tiempo real
totalSuspiciousObjectsFound	Cantidad total de Objetos probablemente infectados detectados desde la hora en que se ejecutó la última tarea de Protección de archivos en tiempo real
totalVirusesFound	Cantidad total de objetos detectados desde la hora en que se ejecutó la última tarea de Protección de archivos en tiempo real
totalObjectsQuarantined	Cantidad total de objetos infectados, objetos infectados y otros objetos que Kaspersky Embedded Systems Security colocó en cuarentena; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsNotQuarantined	Cantidad total de objetos infectados o probablemente infectados que Kaspersky Embedded Systems Security intentó poner en cuarentena, pero no pudo hacerlo; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez

Contador	Definición
totalObjectsDisinfected	Cantidad total de objetos infectados que Kaspersky Embedded Systems Security desinfectó; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsNotDisinfected	Cantidad total de objetos infectados y otros objetos que Kaspersky Embedded Systems Security intentó desinfectar, pero no pudo hacerlo; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsDeleted	Cantidad total de objetos infectados, objetos infectados y otros objetos que Kaspersky Embedded Systems Security desinfectó; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsNotDeleted	Cantidad total de objetos probablemente infectados, objetos infectados y otros objetos que Kaspersky Embedded Systems Security intentó desinfectar, pero no pudo hacerlo; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsBackedUp	Cantidad total de objetos infectados y otros objetos que Kaspersky Embedded Systems Security colocó en Copia de seguridad; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsNotBackedUp	Cantidad total de objetos infectados y otros objetos que Kaspersky Embedded Systems Security intentó colocar en Copia de seguridad, pero no pudo hacerlo; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez

Capturas SNMP de Kaspersky Embedded Systems Security

Las opciones de capturas SNMP en Kaspersky Embedded Systems Security se resume a continuación:

- eventThreatDetected: se ha detectado un objeto.

  Las opciones de la captura se indican a continuación:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty

- eventBackupStorageSizeExceeds: se superó el tamaño máximo de la copia de seguridad. El tamaño total de los datos en la copia de seguridad ha excedido el valor especificado por el **Tamaño máx. de Copia de seguridad (MB)**. Kaspersky Embedded Systems Security continúa realizando copias de seguridad de objetos infectados.

  Las opciones de la captura se indican a continuación:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventThresholdBackupStorageSizeExceeds: Umbral de espacio disponible para la copia de seguridad alcanzado. La cantidad de espacio libre en Copia de seguridad asignado por el **Valor umbral de espacio disponible (MB)** es igual o menor que el valor especificado. Kaspersky Embedded Systems Security continúa realizando copias de seguridad de objetos infectados.

  Las opciones de la captura se indican a continuación:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventQuarantineStorageSizeExceeds: se superó el tamaño máximo de la cuarentena. El tamaño total de los datos en Cuarentena ha superado el valor especificado por el **Tamaño máximo de cuarentena (MB)**. Kaspersky Embedded Systems Security continúa poniendo en cuarentena objetos probablemente infectados.

  Las opciones de la captura se indican a continuación:

  - eventDateAndTime
  - eventSeverity
  - eventSource
- eventObjectNotQuarantined: Error de cuarentena.

  Las opciones de la captura se indican a continuación:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - userName
  - computerName
  - objectName
  - storageObjectNotAddedEventReason
- eventObjectNotBackuped: Error al guardar una copia de objeto en Copia de seguridad.

  Las opciones de la captura se indican a continuación:

  - eventSeverity
  - eventDateAndTime
  - eventSource

  - objectName
  - userName
  - computerName
  - storageObjectNotAddedEventReason
- eventQuarantineInternalError: Error interno de la cuarentena.

  Las opciones de la captura se indican a continuación:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventBackupInternalError: Error de Copia de seguridad.

  Las opciones de la captura se indican a continuación:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventAVBasesOutdated: La base de datos antivirus está desactualizada. Se está calculando la cantidad de días desde la última ejecución de la tarea de actualización de bases de datos (tarea local o tarea de grupo, o tarea para conjuntos de equipos).

  Las opciones de la captura se indican a continuación:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - días
- eventAVBasesTotallyOutdated: La base de datos antivirus es obsoleta. Se está calculando la cantidad de días desde la última ejecución de la tarea de actualización de bases de datos (tarea local o tarea de grupo, o tarea para conjuntos de equipos).

  Las opciones de la captura se indican a continuación:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - días

- eventApplicationStarted: Kaspersky Embedded Systems Security se está ejecutando.

  Las opciones de la captura se indican a continuación:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventApplicationShutdown: Kaspersky Embedded Systems Security está detenido.

  Las opciones de la captura se indican a continuación:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventCriticalAreasScanWasntPerformForALongTime: Las áreas críticas no se han analizado durante un periodo prolongado. Calculado como la cantidad de días desde la última finalización de la tarea de Análisis de áreas críticas.

  Las opciones de la captura se indican a continuación:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - días
- eventLicenseHasExpired: La licencia ha caducado.

  Las opciones de la captura se indican a continuación:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventLicenseExpiresSoon: La licencia expira pronto. Calculado como la cantidad de días hasta la fecha de caducidad de la licencia.

  Las opciones de la captura se indican a continuación:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - días
- eventTaskInternalError: La tarea finalizó con un error.

  Las opciones de la captura se indican a continuación:

  - eventSeverity
  - eventDateAndTime
  - eventSource

    - errorCode
    - knowledgeBaseId
    - taskName
- eventUpdateError: Error de rendimiento de tareas de actualización.

  Las opciones de la captura se indican a continuación:

    - eventSeverity
    - eventDateAndTime
    - taskName
    - updaterErrorEventReason

Las descripciones de las opciones de capturas y sus valores de parámetro posibles son las siguientes:

- eventDateAndTime: fecha y hora del evento.
- eventSeverity: nivel de importancia.

  La opción puede tener los siguientes valores:

    - critical (1): crítico
    - warning (2): advertencia
    - info (3): informativo
- userName: un nombre de usuario (por ejemplo, nombre de usuario que intentó acceder a un archivo infectado).
- computerName: nombre del equipo (por ejemplo, nombre del equipo desde el que se intentó acceder a un archivo infectado).
- eventSource: componente funcional donde se generó el evento.

  La opción puede tener los siguientes valores:

    - unknown (0): componente funcional no conocido
    - quarantine (1): cuarentena
    - backup (2): Copia de seguridad
    - reporting (3): registros de tareas
    - updates (4): actualización
    - realTimeProtection (5): protección de archivos en tiempo real
    - onDemandScanning (6): análisis a pedido
    - product (7): evento relacionado con la operación de Kaspersky Embedded Systems Security en su totalidad en lugar de estar relacionado con operaciones de componentes individuales
    - systemAudit (8): registro de auditoría del sistema
- eventReason: el activador del evento, lo que provocó el evento.

La opción puede tener los siguientes valores:

- reasonUnknown(0): se desconoce el motivo
- reasonInvalidSettings (1): solo para los eventos de copia de seguridad y cuarentena, se muestra si la cuarentena o la copia de seguridad no están disponibles (permisos de acceso insuficientes o la carpeta está especificada de manera incorrecta en la Configuración de cuarentena, por ejemplo, se especificó una ruta de red). En este caso, Kaspersky Embedded Systems Security utilizará la carpeta de Copia de seguridad o de Cuarentena predeterminada.

- objectName: un nombre de objeto (por ejemplo, nombre del archivo donde se detectó el virus).
- threatName: El nombre del objeto según la clasificación de la Enciclopedia de Virus https://encyclopedia.kaspersky.com/knowledge/classification/. Este nombre se incluye en el nombre completo del objeto detectado en los resultados de detección de objetos de Kaspersky Embedded Systems Security. Puede ver el nombre completo de un objeto detectado en el registro de tareas (consulte la sección “Configuración del registro”, en la página 100).
- detectType: tipo de objeto detectado.

  La opción puede tener los siguientes valores:

  - undefined (0): sin definir
  - virware: virus habituales y gusanos de red
  - trojware: troyanos
  - malware: otros programas maliciosos
  - adware: software de publicidad
  - pornware: software pornográfico
  - riskware: aplicaciones legítimas que utilizan los intrusos para dañar el equipo o los datos personales del usuario
- detectCertainty: nivel de certeza de detección de amenaza.

  La opción puede tener los siguientes valores:

  - Sospecha (probablemente infectado): Kaspersky Embedded Systems Security ha detectado una coincidencia parcial entre una sección del código del objeto y la sección del código malicioso conocido
  - Seguro (infectado): Kaspersky Embedded Systems Security ha detectado una coincidencia completa entre una sección del código del objeto y la sección del código malicioso conocido,
- days: cantidad de días (por ejemplo, la cantidad de días hasta la fecha de caducidad de la licencia).
- errorCode: un código de error.
- knowledgeBaseId: dirección de un artículo de la base de conocimientos (por ejemplo, dirección del artículo que explica un error en particular).
- taskName: un nombre de la tarea.
- updaterErrorEventReason: motivo del error de actualización.

  La opción puede tener los siguientes valores:

  - reasonUnknown(0): se desconoce el motivo
  - reasonAccessDenied: acceso denegado
  - reasonUrlsExhausted: se agotó la lista de orígenes de actualizaciones

- reasonInvalidConfig: archivo de configuración no válido
- reasonInvalidSignature: firma no válida
- reasonCantCreateFolder: no se puede crear la carpeta
- reasonFileOperError: error de archivo
- reasonDataCorrupted: el objeto está dañado
- reasonConnectionReset: conexión restablecida
- reasonTimeOut: se excedió el tiempo de espera de conexión
- reasonProxyAuthError: error de autenticación de proxy
- reasonServerAuthError: error de autenticación del servidor
- reasonHostNotFound: no se encuentra el equipo
- reasonServerBusy: servidor no disponible
- reasonConnectionError: error de conexión
- reasonModuleNotFound: no se encontró el objeto
- reasonBlstCheckFailed(16): error al consultar la lista negra de claves. Es posible que se estuvieran publicando actualizaciones de las bases de datos durante la actualización; repita la actualización dentro de unos minutos.

- storageObjectNotAddedEventReason: el motivo por el que no se realizó una copia de seguridad del objeto o no se colocó en cuarentena.

  La opción puede tener los siguientes valores:

  - reasonUnknown(0): se desconoce el motivo
  - reasonStorageInternalError: error de la base de datos; se debe restaurar Kaspersky Embedded Systems Security.
  - reasonStorageReadOnly: la base de datos es de solo lectura; se debe restaurar Kaspersky Embedded Systems Security.
  - reasonStorageIOError: error de entrada-salida: a) Kaspersky Embedded Systems Security está dañado, se debe restaurar Kaspersky Embedded Systems Security; b) el disco con archivos de Kaspersky Embedded Systems Security está dañado.
  - reasonStorageCorrupted: el almacenamiento está dañado; se debe restaurar Kaspersky Embedded Systems Security.
  - reasonStorageFull: la base de datos está llena; se requiere espacio libre en disco.
  - reasonStorageOpenError: no se pudo abrir el archivo de la base de datos; se debe restaurar Kaspersky Embedded Systems Security.
  - reasonStorageOSFeatureError: algunas funciones del sistema operativo no se corresponden con los requisitos de Kaspersky Embedded Systems Security.
  - reasonObjectNotFound: el objeto que se coloca en cuarentena no existe en el disco.
  - reasonObjectAccessError: permisos insuficientes para usar la API de Copia de seguridad: la cuenta que se utiliza para realizar la operación no tiene permisos del operador de Copia de seguridad
  - reasonDiskOutOfSpace: espacio en disco insuficiente

Integración con WMI

Kaspersky Embedded Systems Security admite la integración con Windows Management Instrumentation (WMI): puede usar sistemas cliente que utilicen WMI para recibir datos a través del estándar Web-Based Enterprise Management (WBEM) para recopilar información sobre el estado de Kaspersky Embedded Systems Security y sus componentes.

Cuando se instala Kaspersky Embedded Systems Security, registra el módulo propietario en el sistema, lo que facilita la creación de un espacio de nombre de Kaspersky Embedded Systems Security y de un espacio de nombre WMI en el equipo local. Un espacio de nombre de Kaspersky Embedded Systems Security le permite trabajar con clases e instancias de Kaspersky Embedded Systems Security y sus propiedades.

Los valores de algunas propiedades de instancias dependen de los tipos de tareas.

Tarea no periódica es una tarea de aplicación que no posee límite de tiempo, y puede estar en constante ejecución o detenida. No existe progreso de ejecución existe para estas tareas. Los resultados de la ejecución de la tarea se registran sin parar mientras la tarea se está ejecutando como evento individual (por ejemplo, la detección de un objeto infectado por cualquiera de las tareas de Protección del equipo en tiempo real). Este tipo de tareas se administra mediante las directivas de Kaspersky Security Center.

Tarea periódica es una tarea de aplicación que posee límite de tiempo y posee un progreso de ejecución que se muestra como porcentaje. Los resultados de la tarea se generan después de su finalización, y se representan como un solo elemento o estado de aplicación modificado (por ejemplo, actualización de bases de datos de la aplicación completada, archivos de configuración generados para las tareas de generación de reglas). Se pueden ejecutar varias tareas periódicas del mismo tipo en un solo equipo simultáneamente (tres tareas de Análisis a pedido con diferentes áreas del análisis). Las tareas periódicas se pueden administrar mediante Kaspersky Security Center como tareas de grupo.

Si usa herramientas para generar consultas de espacios de nombre WMI y recibir datos dinámicos de espacios de nombre WMI en una red corporativa, podrá recibir información sobre el estado de la aplicación actual (consulte la tabla a continuación).

Tabla 77. Información sobre el estado de la aplicación

Propiedad de la instancia	Descripción	Valores
ProductName	El nombre de la aplicación instalada.	Nombre completo de aplicación sin número de versión.
ProductVersion	La versión completa de la aplicación instalada	Número completo de la versión de la aplicación, incluido el número de compilación.
InstalledPatches	El grupo de nombres de parches que se implementaron para la aplicación.	La lista de parches críticos instalados para la aplicación.
IsLicenseInstalled	El estado de activación de la aplicación.	El estado de la clave utilizada para activar la aplicación. Valores posibles: • False: no se han configurado una clave o el código de activación en la aplicación. • True: se han agregado una clave o el código de activación en la aplicación.

Propiedad de la instancia	Descripción	Valores
LicenseDaysLeft	Muestra cuántos días restan antes de que caduque la licencia actual.	Número de días restantes antes del vencimiento de la licencia actual. Valores no positivos posibles: • 0 - La licencia ha caducado • -1 - No se pudo obtener información sobre la clave actual, o la clave especificada no puede usarse para activar la aplicación (por ejemplo, se bloquea según una lista negra de claves).
AVBasesDatetime	La marca de fecha y hora para una versión de la base de datos antivirus actual.	Fecha y hora de la creación de las bases de datos antivirus actualmente en uso. Si la aplicación instalada no usa bases de datos antivirus, el campo tiene el valor “No instalada”.
IsExploitPreventionEnabled	El estado del componente Prevención de exploits.	Estado del componente Prevención de exploits. Valores posibles: • True - El componente Prevención de exploits está habilitado y ofrece protección. • False - El componente Prevención de exploits no ofrece protección. Por ejemplo: desactivado, no instalado, se ha infringido el contrato de licencia.
ProtectionTasksRunning	El grupo de tareas de protección que se están ejecutando actualmente.	Enumera las tareas de protección, control y supervisión que se están ejecutando actualmente. Este campo debería explicar todas las tareas no periódicas en ejecución. Si no se está ejecutando ninguna tarea no periódica, el campo tiene el valor "No".
IsAppControlRunning	El estado de la tarea Control de inicio de aplicaciones.	Estado de la tarea Control de inicio de aplicaciones. • True - La tarea Control de inicio de aplicaciones se está ejecutando actualmente. • False - La tarea Control de inicio de aplicaciones no se está ejecutando actualmente o el componente Control de inicio de aplicaciones no está instalado.

Propiedad de la instancia	Descripción	Valores
AppControlMode	El modo de la tarea Control de inicio de aplicaciones.	Descripción del estado actual del componente Control de inicio de aplicaciones que explicita el modo seleccionado para la tarea correspondiente. Valores posibles: • Activo - El modo **Activo** está seleccionado en la configuración de la tarea. • Solo estadísticas - El modo **Solo estadísticas** está seleccionado en la configuración de la tarea. • No instalado - El componente Control de inicio de aplicaciones no está instalado
AppControlRulesNumber	Número total de reglas de control de inicio de aplicaciones.	El número de reglas especificadas actualmente en la configuración de la tarea Control de inicio de aplicaciones.
AppControlLastBlocking	La marca de fecha y hora del último inicio de aplicaciones bloqueado por la tarea Control de inicio de aplicaciones en cualquier modo.	La fecha y la hora en que el componente Control de inicio de aplicaciones bloqueó por última vez el inicio de una aplicación. Este campo incluye todas las aplicaciones bloqueadas, sin tener en cuenta el modo de la tarea. Si no hay ninguna instancia de inicio de aplicaciones bloqueada registrada al momento de procesar la consulta WMI, se asigna el valor “No” al campo.
PeriodicTasksRunning	El grupo de tareas periódicas que se están ejecutando actualmente.	Lista de tareas Análisis a pedido, Actualización y de inventario que se están ejecutando actualmente. Este campo debe incluir todas las tareas periódicas en ejecución. Si no se está ejecutando ninguna tarea periódica actualmente, el campo tiene el valor "No".
ConnectionState	El estado de la conexión entre el componente Proveedor de WMI y el servicio de Kaspersky Security (KAVFS).	Información sobre el estado de la conexión entre el módulo Proveedor de WMI y el servicio de Kaspersky Security. Valores posibles: • Éxito - Se estableció correctamente la conexión: el cliente de WMI puede recibir la información sobre el estado de la aplicación. • Error. Código de error: <código> - La conexión no se pudo establecer debido a un error con el código especificado.

Estos datos representan propiedades de instancias KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security, donde:

- KasperskySecurity_ProductInfo es el nombre de la clase Kaspersky Embedded Systems Security
- .ProductName=Kaspersky Embedded Systems Security es el parámetro de la clave de Kaspersky Embedded Systems Security

La instancia se crea en el espacio de nombre ROOT\Kaspersky\Security.

Cómo utilizar Kaspersky Embedded Systems Security desde la línea de comandos

Esta sección describe cómo utilizar Kaspersky Embedded Systems Security desde la línea de comandos.

En este capítulo

Comandos de la línea de comandos

Puede ejecutar comandos básicos de administración de Kaspersky Embedded Systems Security desde la línea de comandos del equipo protegido, si incluye el componente Utilidad de línea de comandos en la lista de funciones instaladas durante la instalación de Kaspersky Embedded Systems Security.

Si utiliza comandos de la línea de comandos, puede administrar solo aquellas funciones a las que tiene acceso según los permisos asignados a su Kaspersky Embedded Systems Security.

Ciertos comandos de Kaspersky Embedded Systems Security se ejecutan en los modos siguientes:

- Modo síncrono: la administración regresa a la Consola solo después de que la ejecución del comando se ha completado.
- Modo asíncrono: la administración regresa a la Consola inmediatamente después de que el comando se ejecuta.

► *Para interrumpir la ejecución del comando en modo síncrono*

presione el acceso directo del teclado **Ctrl+C**.

Siga las siguientes reglas al introducir comandos de Kaspersky Embedded Systems Security:

- Introduzca modificadores y comandos utilizando mayúsculas y minúsculas.
- Delimite los modificadores con el carácter de espacio.
- Si el nombre del archivo o de la carpeta cuya ruta se especifica como valor de clave contiene un espacio, especifique la ruta del archivo o de la carpeta entre comillas, por ejemplo: `"C:\TEST\test cpp.exe"`
- Si es necesario, use marcadores de posición en las máscaras de ruta de acceso o el nombre de archivo, por ejemplo: “`C:\Temp\Temp*\`”, “`C:\Temp\Temp???.doc`”, “`C:\Temp\Temp*.doc`”

Se puede usar la línea de comandos para todo el rango de operaciones requeridas para la administración de Kaspersky Embedded Systems Security (consulte la tabla a continuación).

Tabla 78. Comandos de Kaspersky Embedded Systems Security

Comando	Descripción
KAVSHELL APPCONTROL (consulte la sección “Cómo completar la lista de reglas de Control de inicio de aplicaciones KAVSHELL APPCONTROL”, en la página 500)	Renueva la lista de reglas especificadas según el principio de adición seleccionado.
KAVSHELL APPCONTROL /CONFIG (consulte la sección “Administración de la tarea Control de inicio de aplicaciones KAVSHELL APPCONTROL /CONFIG”, en la página 497)	Controla el modo de operación de la tarea Control de inicio de aplicaciones
KAVSHELL APPCONTROL /GENERATE (consulte la sección “Generador de reglas para Control de inicio de aplicaciones KAVSHELL APPCONTROL /GENERATE”, en la página 498)	Inicia la tarea de Generador de reglas para Control de inicio de aplicaciones.
KAVSHELL VACUUM (consulte la sección "Desfragmentación de archivos de registro de Kaspersky Embedded Systems Security. KAVSHELL VACUUM”, en la página 508)	Desfragmenta los archivos de registro de Kaspersky Embedded Systems Security.
KAVSHELL PASSWORD	Administra la configuración de protección con contraseña.
KAVSHELL HELP (consulte la sección “Visualización de la ayuda de comandos de Kaspersky Embedded Systems Security. KAVSHELL HELP”, en la página 489)	Muestra la ayuda de comandos de Kaspersky Embedded Systems Security.
KAVSHELL START (consulte la sección “Inicio y detención del servicio de Kaspersky Security KAVSHELL START, KAVSHELL STOP”, en la página 490)	Inicia el servicio de Kaspersky Embedded Systems Security.
KAVSHELL STOP (consulte la sección “Inicio y detención del servicio de Kaspersky Security KAVSHELL START, KAVSHELL STOP”, en la página 490)	Detiene el servicio de Kaspersky Embedded Systems Security.
KAVSHELL SCAN (consulte la sección “Análisis del área seleccionada. KAVSHELL SCAN”, en la página 490)	Crea e inicia una tarea de Análisis a pedido temporal con la configuración de seguridad y de área del análisis determinada por los modificadores de comando.
KAVSHELL SCANCRITICAL (consulte la sección “Inicio de la tarea Análisis de áreas críticas. KAVSHELL SCANCRITICAL”, en la página 494)	Inicia la tarea del sistema Análisis de áreas críticas.
KAVSHELL TASK (consulte la sección “Administración de tarea especificada de manera asíncrona. KAVSHELL TASK”, en la página 495)	Inicia/pausa/reanuda/detiene la tarea seleccionada de manera asíncrona/muestra el estado de tarea actual/muestra estadísticas.
KAVSHELL RTP (consulte la sección “Inicio y detención de tareas de protección en tiempo real. KAVSHELL RTP”, en la página 497)	Inicia o detiene todas las tareas de protección en tiempo real.
KAVSHELL UPDATE (consulte la sección “Inicio de la tarea de actualización de bases de datos de Kaspersky Embedded Systems Security. KAVSHELL UPDATE”, en la página 502)	Inicia la tarea de actualización de las bases de datos de Kaspersky Embedded Systems Security con la configuración especificada mediante modificadores de comando.

Comando	Descripción
KAVSHELL ROLLBACK (consulte la sección “Reversión de actualizaciones de bases de datos de Kaspersky Embedded Systems Security. KAVSHELL ROLLBACK”, en la página 506)	Revierte las bases de datos a la versión anterior.
KAVSHELL LICENSE	Agrega o elimina las claves. Visualiza información sobre las claves agregadas.
KAVSHELL TRACE (consulte la sección “Habilitación, configuración y deshabilitación del registro de rastreo. KAVSHELL TRACE”, en la página 507)	Habilita o deshabilita el registro de rastreo, administra la configuración del registro de rastreo.
KAVSHELL DUMP (consulte la sección “Habilitación y deshabilitación de la creación de archivos de volcado. KAVSHELL DUMP”, en la página 510)	Habilita o deshabilita los archivos de volcado de memoria de Kaspersky Embedded Systems Security en caso de interrupción anormal de los procesos.
KAVSHELL IMPORT (consulte la sección “Importación de la configuración. KAVSHELL IMPORT”, en la página 511)	Importa valores de configuración, funciones y tareas generales de Kaspersky Embedded Systems Security de un archivo de configuración creado con antelación.
KAVSHELL EXPORT (consulte la sección “Exportación de configuración. KAVSHELL EXPORT”, en la página 512)	Exporta todos los valores de configuración de Kaspersky Embedded Systems Security y tareas existentes a un archivo de configuración.
KAVSHELL DEVCONTROL (consulte la sección “Cómo completar la lista de reglas de Control de dispositivos. KAVSHELL DEVCONTROL”, en la página 501)	Agrega a la lista de reglas de control de dispositivos generadas según el método seleccionado.

Visualización de la ayuda de comandos de Kaspersky Embedded Systems Security. KAVSHELL HELP

Para obtener la lista de todos los comandos de Kaspersky Embedded Systems Security, ejecute uno de los comandos siguientes:

```
/KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Para obtener una descripción de un comando y su sintaxis, ejecute uno de los siguientes comandos:

```
KAVSHELL HELP <comando>

KAVSHELL <comando> /?
```

Ejemplos del comando KAVSHELL HELP

Para ver información detallada sobre el comando KAVSHELL SCAN, ejecute el siguiente comando:

```
KAVSHELL HELP SCAN
```

Inicio y detención del servicio de Kaspersky Security KAVSHELL START, KAVSHELL STOP

Para ejecutar el servicio de Kaspersky Security, ejecute el comando

```
KAVSHELL START
```

De manera predeterminada, cuando se inicia el servicio de Kaspersky Security, se inician las tareas de protección de archivos en tiempo real y análisis cuando arranca el sistema, así como las demás tareas cuyo inicio esté programado **Al inicio de la aplicación**.

Para detener el servicio de Kaspersky Security, ejecute el comando

```
KAVSHELL STOP
```

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Análisis del área seleccionada. KAVSHELL SCAN

Para iniciar una tarea de análisis de áreas específicas del equipo protegido, utilice el comando `KAVSHELL SCAN`. Los modificadores del comando especifican el área del análisis y la configuración de seguridad del nodo seleccionado.

La tarea Análisis a pedido iniciada con el comando `KAVSHELL SCAN` es una tarea temporal. Se muestra en Consola de la aplicación solo al ejecutarse (no se puede ver la configuración de la tarea en la Consola de la aplicación). Al mismo tiempo, se genera el registro de rendimiento de tareas. Se muestra en los **Registros de tareas** de la Consola de la aplicación.

Al especificar las rutas de acceso en las tareas de análisis de áreas específicas, se pueden utilizar las variables del entorno. Si se utilizan las variables del entorno especificadas para el usuario, ejecute el comando `KAVSHELL SCAN` con los permisos para ese usuario.

El comando `KAVSHELL SCAN` se ejecuta en el modo síncrono.

Para iniciar una tarea Análisis a pedido desde la línea de comandos, use el comando KAVSHELL TASK (consulte la sección “Administración de la tarea especificada de manera asíncrona. KAVSHELL TASK”, en la página 495).

Sintaxis del comando KAVSHELL SCAN

```
KAVSHELL SCAN <área del análisis>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:< ruta de acceso al
archivo con la lista de áreas del análisis >] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>]
[/EM:<”masks”>] [/ES:<tamaño>] [/ET:<cantidad de segundos>] [/TZOFF]
[/OF:<SKIP|RESIDENT|SCAN[=<días>] [NORECALL]>]
[/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<ruta de acceso al
```

```
archivo de registro de tareas>] [/ANSI] [/ALIAS:<alias de la tarea>]
```

El comando KAVSHELL SCAN tiene claves obligatorias y opcionales (consulte la tabla a continuación).

Ejemplos del comando KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe
"\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA
/E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1
/NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Tabla 79. Modificadores del comando KAVSHELL SCAN

Clave	Descripción
Área del análisis. Modificador obligatorio.	
<archivos>	Especifica el área del análisis: lista de archivos, carpetas, rutas de red y áreas predefinidas. Especifique rutas de red en el formato UNC (convención de nomenclatura universal). En el siguiente ejemplo, la carpeta Folder4 se especifica sin una ruta de acceso y está ubicada en la carpeta desde la cual se ejecuta el comando KAVSHELL: KAVSHELL SCAN Folder4 Si el nombre del objeto a comprobar tiene espacios, se debe colocar entre signos de interrogación. Cuando se selecciona una carpeta, Kaspersky Embedded Systems Security también comprobará todas las subcarpetas de la carpeta en cuestión. Los símbolos * o ? se pueden utilizar para analizar un grupo de archivos.
<carpetas>	
<ruta de red>	
/MEMORY	Analizar objetos en RAM
/SHARED	Analizar carpetas compartidas en el equipo
/STARTUP	Analizar objetos de ejecución automática
/REMDRIVES	Analizar unidades extraíbles
/FIXDRIVES	Analizar unidades de disco duro
/MYCOMP	Analizar todas las áreas del equipo protegido
/L:<ruta del archivo con la lista de áreas del análisis>	Nombre de archivo con la lista de áreas de análisis incluida la ruta completa para el archivo. Delimite áreas de análisis en los archivos utilizando saltos de línea. Puede especificar áreas de análisis predefinidas como se muestra a continuación en este ejemplo de un archivo con una lista de áreas del análisis: C:\ D:\Docs*.doc E:\Mis documentos /STARTUP /SHARED

Clave	Descripción
Objetos analizados (tipos de archivos). Si no especifica valores para este modificador, Kaspersky Embedded Systems Security analizará los objetos por formato.	
/FA	Analizar todos los objetos
/FC	Analizar los objetos por formato (de manera predeterminada). Kaspersky Embedded Systems Security analiza solo objetos cuyos formatos figuran en la lista de formatos de objetos infectables.
/FE	Analizar los objetos por extensión Kaspersky Embedded Systems Security analiza solo objetos con extensiones que figuran en la lista de extensiones de objetos infectables.
/NEWONLY	Analizar solo los archivos nuevos y modificados. Si no indica este modificador, Kaspersky Embedded Systems Security analizará todos los objetos.
Acción que se realizará con los objetos infectados y otros objetos. Si no se especificaron valores para este modificador, Kaspersky Embedded Systems Security ejecutará la acción **Omitir**.	
DISINFECT	Desinfectar, omitir si la desinfección es imposible Los valores de configuración DISINFECT y DELETE se guardan en la versión actual de Kaspersky Embedded Systems Security a fin de asegurar compatibilidad con versiones anteriores. Esos valores se pueden utilizar en lugar de los comandos de modificador /AI: y /AS: En ese caso, Kaspersky Embedded Systems Security no procesará objetos probablemente infectados.
DISINFDEL	Desinfectar, eliminar si la desinfección es imposible
DELETE	Eliminar Los valores de configuración DISINFECT y DELETE se guardan en la versión actual de Kaspersky Embedded Systems Security a fin de asegurar compatibilidad con versiones anteriores. Esos valores se pueden utilizar en lugar de los comandos de modificador /AI: y /AS: En ese caso, Kaspersky Embedded Systems Security no procesará objetos probablemente infectados.
REPORT	Enviar un informe (de manera predeterminada)
AUTO	Ejecutar la acción recomendada
/AS: **Acción que se realizará con los objetos probablemente infectados**/ Si no se especificaron valores para este modificador, Kaspersky Embedded Systems Security ejecutará la acción **Omitir**.	
CUARENTENA	Cuarentena
DELETE	Eliminar
REPORT	Enviar un informe (de manera predeterminada)
AUTO	Ejecutar la acción recomendada
Exclusiones	

Clave	Descripción
/E:ABMSPO	Excluye objetos compuestos de los siguientes tipos: A: archivos (se analizan solo los archivos SFX) B: bases de datos de correo electrónico M: correo electrónico sin formato S: archivos y archivos SFX P: objetos empaquetados O: objetos OLE integrados
/EM:<″masks″>	Excluir archivos por máscara Se pueden especificar varias máscaras, por ejemplo: EM:″*.txt; *.png; C\Videos*.avi″.
/ET:<cantidad de segundos>	Detener el procesamiento de un objeto si demora más tiempo que la cantidad de segundos especificada en el valor <cantidad de segundos>. No hay restricciones de tiempo de manera predeterminada.
/ES:<tamaño>	No analizar objetos compuestos que superan el tamaño (en MB) especificado por el valor <tamaño>. Kaspersky Embedded Systems Security analiza objetos de todo tamaño de manera predeterminada.
/TZOFF	Deshabilitar exclusiones de zonas de confianza
Configuración avanzada (Opciones)	
/NOICHECKER	Deshabilitar la utilización de iChecker (habilitada de forma predeterminada).
/NOISWIFT	Deshabilitar la utilización de iSwift (habilitada de forma predeterminada).
/ANALYZERLEVEL:<intensidad de análisis>	Habilitar el Analizador heurístico, configurar el nivel de análisis. Los siguientes niveles de análisis heurístico están disponibles: 1: ligero 2: medio 3: profundo Si se omite el modificador, Kaspersky Embedded Systems Security no utilizará el analizador heurístico.
/ALIAS:<alias de la tarea>	Permite asignar un nombre temporal a una tarea de Análisis a pedido por el cual se puede acceder a la tarea durante su ejecución; por ejemplo, para ver sus estadísticas con el comando TASK. El alias de tarea debe ser único entre los alias de tarea de todos los componentes funcionales de Kaspersky Embedded Systems Security. Si no se especificó este modificador, se utiliza el nombre temporal scan_<pid_de_kavshell>, por ejemplo, scan_1234. En la Consola de la aplicación, se asigna a la tarea el nombre Analizar objetos (<fecha y hora>), por ejemplo, Analizar objetos 16/08/2007 5:13:14 p. m.
Configuración de registros de tareas (configuración de informes)	

Clave	Descripción
/W:<ruta del archivo de registro de tareas>	Si se especifica esta clave, Kaspersky Embedded Systems Security guardará el archivo de registro de tareas con el nombre definido por el valor de la clave. El archivo de registro contiene las estadísticas de ejecución, la hora de inicio y finalización (detención) de la tarea, e información sobre los eventos producidos en ella. El registro se utiliza para registrar eventos definidos por la configuración de los registros de tareas y el registro de eventos de Kaspersky Embedded Systems Security en el Visor de eventos. Se puede especificar la ruta relativa o absoluta del archivo de registro. Si se especifica solo el nombre de un archivo sin especificar la ruta correspondiente, el archivo de registro se creará en la carpeta actual. Si se reinicia el comando con la misma configuración de registro, se sobrescribirá el archivo de registro existente. Se puede visualizar el archivo de registro mientras se ejecuta una tarea. El registro se muestra en el nodo Registros de tareas de la Consola de la aplicación. Si se produce un error en Kaspersky Embedded Systems Security al crear el archivo de registro, esto no evitará que el comando se ejecute, pero se mostrará un mensaje de error.
/ANSI	La opción permite la grabación de los eventos en el registro de tareas en la codificación ANSI. La opción ANSI no se aplicará si la opción W no está definida. Si no se especificó la opción ANSI, el registro de tareas se genera con la codificación UNICODE.

Iniciar la tarea Análisis de áreas críticas. KAVSHELL SCANCRITICAL

Use el comando `KAVSHELL SCANCRITICAL` para iniciar el Análisis de áreas críticas de la tarea de Análisis a pedido del sistema con la configuración definida en la Consola de la aplicación.

Sintaxis del comando KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<ruta del archivo del registro de tareas>]
```

Ejemplos del comando KAVSHELL SCANCRITICAL

Para ejecutar la tarea Análisis a pedido de Análisis de áreas críticas y guardar el registro de tareas scancritical.log en la carpeta actual, ejecute el siguiente comando:

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Según la sintaxis del modificador /W, se puede configurar la ubicación del registro de tareas (consulte la tabla a continuación).

Tabla 80. Sintaxis del modificador /W para el comando KAVSHELL SCANCRITICAL

Clave	Descripción

Clave	Descripción
/W:<ruta del archivo de registro de tareas>	Si se especifica esta clave, Kaspersky Embedded Systems Security guardará el archivo de registro de tareas con el nombre definido por el valor de la clave. El archivo de registro contiene las estadísticas de ejecución, la hora de inicio y finalización (detención) de la tarea, e información sobre los eventos producidos en ella. El registro se utiliza para registrar eventos definidos por la configuración de los registros de tareas y el Registro de eventos de la aplicación en el Visor de eventos. Se puede especificar la ruta relativa o absoluta del archivo de registro. Si se especifica solo el nombre de un archivo sin especificar la ruta correspondiente, el archivo de registro se creará en la carpeta actual. Si se reinicia el comando con la misma configuración de registro, se sobrescribirá el archivo de registro existente. Se puede visualizar el archivo de registro mientras se ejecuta una tarea. El registro se muestra en el nodo **Registros de tareas** de la Consola de la aplicación. Si se produce un error en Kaspersky Embedded Systems Security al crear el archivo de registro, esto no evitará que el comando se ejecute, pero se mostrará un mensaje de error.

Administración de una tarea especificada asíncronamente. KAVSHELL TASK

La utilización del comando `KAVSHELL TASK` le permite administrar la tarea especificada: ejecutar, pausar, reanudar y detener la tarea especificada y ver el estado y estadísticas de la tarea actual. El comando se ejecuta en modo asíncrono.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL TASK

```
KAVSHELL TASK [<alias de nombre de tarea> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Ejemplos del comando KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE
```

El comando `KAVSHELL TASK` se puede ejecutar sin modificadores o con uno o varios modificadores (consulte la

tabla a continuación).

Tabla 81. Modificadores del comando KAVSHELL TASK

Clave	Descripción
Sin claves	Devuelve la lista de todas las tareas existentes de Kaspersky Embedded Systems Security. La lista contiene los campos: nombre alternativo de la tarea, categoría de la tarea (del sistema o personalizada) y estado de la tarea actual.
<alias de tarea>	En lugar del nombre de la tarea, en el comando SCAN TASK use el alias de tarea, un nombre corto adicional que Kaspersky Embedded Systems Security asigna a las tareas. Para ver los alias de tarea de Kaspersky Embedded Systems Security, introduzca el comando KAVSHELL TASK sin ningún modificador.
/START	Inicia la tarea especificada en modo asíncrono.
/STOP	Detiene la tarea especificada.
/PAUSE	Pone en pausa la tarea especificada.
/RESUME	Reanuda la tarea especificada en modo asíncrono.
/STATE	Muestra el estado de la tarea actual (por ejemplo, *En ejecución*, *Completada*, *En pausa*, *Detenida*, *Error*, *Iniciando* o *Recuperando*).
/STATISTICS	Recupera las estadísticas de la tarea: información acerca de la cantidad de objetos procesados desde el inicio de la tarea hasta la actualidad.

Tenga en cuenta que no todas las tareas de Kaspersky Embedded Systems Security son totalmente compatibles con estas claves.

Códigos de devolución para el comando KAVSHELL TASK (consulte la sección “Códigos de devolución para el comando KAVSHELL TASK”, en la página 515).

Registro de KAVFS como un proceso de protección de sistemas. KAVSHELL CONFIG

El comando `CONFIG KAVSHELL` le permite controlar el registro del Servicio de Kaspersky Security como un proceso de protección de sistemas (Protected Process Light) mediante el controlador ELAM, instalado en el sistema operativo durante la instalación de la aplicación.

Sintaxis del comando KAVSHELL CONFIG

```
KAVSHELL CONFIG/PPL: <ON|OFF>
```

Tabla 82. Claves del comando KAVSHELL CONFIG

Clave	Descripción
/PPL:ON	Registrar el Servicio de Kaspersky Security como PPL.
/PPL:OFF	Eliminar el atributo PPL para el Servicio de Kaspersky Security.

La aplicación realiza automáticamente la anulación del registro de servicio cuando se lleva a cabo cualquiera de

las siguientes acciones:

- desinstalación de la aplicación
- actualización de la aplicación
- instalación de parches
- reparación de componentes de la aplicación

Códigos de devolución para el comando KAVSHELL CONFIG.

Inicio y detención de tareas de protección en tiempo real. KAVSHELL RTP

El comando `KAVSHELL RTP` se puede utilizar para iniciar o detener todas las tareas de Protección en tiempo real.

> Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL RTP

```
KAVSHELL RTP {/START | /STOP}
```

Ejemplo del comando KAVSHELL RTP

Para iniciar todas las tareas de Protección en tiempo real, ejecute el siguiente comando:

```
KAVSHELL RTP /START
```

El comando `KAVSHELL RTP` puede incluir cualquiera de los dos modificadores obligatorios (consulte la tabla a continuación).

Tabla 83. Modificadores del comando KAVSHELL RTP

Clave	Descripción
/START	Inicia todas las tareas de Protección en tiempo real: Protección de archivos en tiempo real y Uso de KSN.
/STOP	Detiene todas las tareas de Protección en tiempo real.

Administración de la tarea Control de inicio de aplicaciones KAVSHELL APPCONTROL /CONFIG

Puede usar el comando `KAVSHELL APPCONTROL /CONFIG` para configurar el modo en el cual la tarea Control de inicio de aplicaciones se ejecuta y supervisa la carga de módulos DLL.

Sintaxis del comando KAVSHELL APPCONTROL /CONFIG

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config
```

/savetofile:<ruta completa al archivo XML>

Ejemplos del comando KKAVSHELL APPCONTROL /CONFIG

► *Para ejecutar la tarea Control de inicio de aplicaciones en el modo **Activo** sin cargar DLL y guardar la configuración de la tarea después de la finalización, ejecute el siguiente comando:*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

Puede ajustar la configuración de la tarea de Control de inicio de aplicaciones usando los parámetros de la línea de comandos (ver la tabla a continuación).

Tabla 84. Modificadores de comando KAVSHELL APPCONTROL /GENERATE

Clave	Descripción
/mode:<applyrules|statistics>	Modo de operación de la tarea Control de inicio de aplicaciones. Puede seleccionar uno de los siguientes modos: • active: aplicar reglas de Control de inicio de aplicaciones; • statistics: solo estadísticas.
/dll:<no|yes>	Habilitar o deshabilitar la supervisión de la carga de DLL.
/savetofile: <ruta de acceso al archivo XML>	Exportar determinadas reglas en el archivo indicado en formato XML.
/savetofile: <el nombre completo al archivo xml>	Guardar la lista de reglas en el archivo.
/savetofile: <el nombre completo al archivo xml> /sdc	Guardar la lista de reglas de Control de distribución de software en el archivo.
/clearsdc	Eliminar todas las reglas de control de distribución de software de la lista.

Generador de reglas para Control de inicio de aplicaciones KAVSHELL APPCONTROL /GENERATE

Con el comando KAVSHELL APPCONTROL /GENERATE puede generar listas de reglas de Control de inicio de aplicaciones.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave [/pwd:<contraseña>].

Sintaxis del comando KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL /GENERATE <ruta de acceso a la carpeta> | /source:<ruta de
acceso a archivos con lista de carpetas> [/masks:<edms>] [/runapp]
```

```
[/rules:<ch|cp|h>] [/strong] [/user:<usuario o grupo de usuarios>] [/export:<ruta de acceso a archivo XML>] [/import:<a|r|m>] [/prefix:<prefijo para nombres de reglas>] [/unique]
```

Ejemplos del comando KAVSHELL APPCONTROL /GENERATE

- *Para generar reglas para archivos desde carpetas especificadas, ejecute el siguiente comando:*

  ```
  KAVSHELL APPCONTROL /GENERATE
  /source:c\folderslist.txt/export:c:\rules\appctrlrules.xml
  ```

- *Para generar reglas para archivos ejecutables de todas las extensiones disponibles en la carpeta especificada y, después de la finalización de la tarea, guardar las reglas generadas en el archivo XML del archivo especificado, ejecute el siguiente comando:*

  ```
  KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms
  /export:c\rules\appctrlrules.xml
  ```

Según la sintaxis de las claves, puede configurar la generación automática de reglas para la tarea Control de inicio de aplicaciones (consulte la tabla a continuación).

Tabla 85. Claves del comando KAVSHELL APPCONTROL /GENERATE

Clave	Descripción
Área de aplicación de las reglas de autorización	
<ruta de acceso a la carpeta>	Especifica la ruta de acceso a la carpeta con los archivos ejecutables que requieren reglas de autorización generadas automáticamente.
/source: <ruta de acceso al archivo con la lista de carpetas>	Especifica la ruta de acceso al archivo TXT con la lista de carpetas que contienen archivos ejecutables que requieren reglas de autorización generadas automáticamente.
/masks: <edms>	Especifica extensiones de archivos ejecutables que requieren reglas de autorización generadas automáticamente. Puede incluir archivos del área de aplicación de las reglas con las siguientes extensiones: • e: archivos EXE • d: archivos DLL • m: archivos MSI • s: scripts
/runapp	Al generar reglas de autorización, tenga en cuenta aplicaciones que se ejecuten en un equipo protegido en el momento de la realización de la tarea.
Acciones al generar automáticamente reglas de autorización	

Clave	Descripción
/rules: <ch|cp|h>	Especifica acciones para realizar durante la generación de reglas de autorización del Control de inicio de aplicaciones: • ch: usar un certificado digital. De no haber un certificado, usar hash SHA256. • cp: usar un certificado digital. De no haber un certificado, usar la ruta al archivo ejecutable. • h: usar hash SHA256.
/strong	Use el asunto y la huella del certificado digital al generar automáticamente las reglas de autorización de Control de inicio de aplicaciones. El comando se ejecuta si se especifica la clave /rules: <ch|cp>.
/user: <usuario o grupo de usuarios>	Especifica el nombre de usuario o un grupo de usuarios para los cuales se aplicarán las reglas. La aplicación supervisará las aplicaciones ejecutadas por el usuario especificado o el grupo de usuarios.
Acciones después de la finalización de Generador de reglas para Control de inicio de aplicaciones	
/export: <ruta de acceso al archivo XML>	Guarda las reglas generadas en un archivo XML.
/unique	Agrega información sobre el equipo con aplicaciones instaladas que son la base para la generación de reglas de autorización del Control de inicio de aplicaciones.
/prefix: <prefijo para nombres de reglas>	Especifica el prefijo del nombre para generar reglas de autorización del control de inicios de aplicaciones.
/import: <a|r|m>	Importa las reglas generadas a la lista de reglas de control de inicio de aplicaciones especificadas según el principio de adición seleccionado. • a: **Agregar a reglas existentes** (las reglas con la configuración idéntica se duplican) • r: **Reemplazar reglas existentes** (las reglas con parámetros idénticos no se agregan; la regla se agrega si al menos un parámetro de la regla es único) • m: **Combinar con reglas existentes** (las reglas con parámetros idénticos no se agregan; la regla se agrega si al menos un parámetro de la regla es único)

Cómo completar la lista de reglas de Control de inicio de aplicaciones KAVSHELL APPCONTROL

Mediante `KAVSHELL APPCONTROL`, se pueden agregar reglas del archivo XML a la lista de reglas de la tarea de Control de inicio de aplicaciones según el principio seleccionado y también se pueden eliminar todas las reglas definidas de la lista.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <ruta de acceso al archivo XML> | /replace <ruta de acceso al archivo XML> | /merge <ruta de acceso al archivo XML> | /clear
```

Ejemplo del comando KAVSHELL APPCONTROL

► *Para agregar reglas de un archivo XML a reglas ya especificadas para la tarea Control de inicio de aplicaciones según el principio Agregar a reglas existentes, ejecute el siguiente comando:*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

Según la sintaxis de las claves, puede seleccionar el principio para agregar reglas nuevas a un archivo XML especificado para una lista de reglas definidas de Control de inicio de aplicaciones (consulte la tabla a continuación).

Tabla 86. Claves del comando `KAVSHELL APPCONTROL`

Clave	Descripción
/append <ruta de acceso al archivo XML>	Renueva la lista de reglas de Control de inicio de aplicaciones según un archivo XML especificado. Principio de adición: **Agregar a reglas existentes** (las reglas con la configuración idéntica se duplican).
/replace <ruta de acceso al archivo XML>	Renueva la lista de reglas de Control de inicio de aplicaciones según un archivo XML especificado. Principio de adición: **Reemplazar reglas existentes** (las reglas con parámetros idénticos no se agregan; la regla se agrega si al menos un parámetro de la regla es único).
/merge <ruta de acceso al archivo XML>	Renueva la lista de reglas de Control de inicio de aplicaciones según un archivo XML especificado. Principio de adición: **Combinar con reglas existentes** (las nuevas reglas no duplican reglas ya definidas).
/clear	Vacía la lista de reglas de Control de inicio de aplicaciones.

Llenado de la lista de reglas de Control de dispositivos. KAVSHELL DEVCONTROL

Mediante `KAVSHELL DEVCONTROL` se pueden agregar reglas del archivo XML a la lista de reglas de la tarea de Control de dispositivos según el principio seleccionado y también se pueden eliminar todas las reglas definidas de

la lista.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <ruta de acceso al archivo XML> | /replace <ruta de acceso al archivo XML> | /merge <ruta de acceso al archivo XML> | /clear
```

Ejemplo del comando KAVSHELL DEVCONTROL

► *Para agregar reglas de un archivo XML a reglas ya especificadas para la tarea de Control de dispositivos según **Agregar a reglas existentes**, ejecute el siguiente comando:*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

Según la sintaxis de las claves, puede seleccionar el principio para agregar reglas nuevas de un archivo XML especificado a una lista de reglas definidas de Control de dispositivos (consulte la tabla a continuación).

Tabla 87. Claves del comando KAVSHELL DEVCONTROL

Clave	Descripción
/append <ruta de acceso al archivo XML>	Renueva la lista de reglas de Control de dispositivos según un archivo XML especificado. Principio de adición: **Agregar a reglas existentes** (las reglas con la configuración idéntica se duplican).
/replace <ruta de acceso al archivo XML>	Renueva la lista de reglas de Control de dispositivos según un archivo XML especificado. Principio de adición: **Reemplazar reglas existentes** (las reglas con parámetros idénticos no se agregan; la regla se agrega si al menos un parámetro de la regla es único).
/merge <ruta de acceso al archivo XML>	Renueva la lista de reglas de Control de dispositivos según un archivo XML especificado. Principio de adición: **Combinar con reglas existentes** (las nuevas reglas no duplican reglas ya definidas).
/clear	Vacía la lista de reglas de Control de dispositivos.

Inicio de tarea de actualización de bases de datos de Kaspersky Embedded Systems Security. KAVSHELL UPDATE

El comando `KAVSHELL UPDATE` se puede utilizar para iniciar el comando de actualización de la base de datos de Kaspersky Embedded Systems Security en modo sincrónico.

La tarea de actualización de bases de datos de Kaspersky Embedded Systems Security ejecutada mediante un comando `KAVSHELL UPDATE` es una tarea temporal. Solo se muestra en la Consola de la aplicación mientras está en ejecución. Al mismo tiempo, se genera el registro de tareas. Se muestra en los **Registros de tareas** de la

Consola de la aplicación. Se pueden aplicar directivas de Kaspersky Security Center para actualizar tareas creadas e iniciadas mediante el comando `KAVSHELL UPDATE` y para actualizar tareas creadas en la Consola de la aplicación. Para información sobre administrar Kaspersky Embedded Systems Security en equipos con Kaspersky Security Center, consulte la sección "Administrar Kaspersky Embedded Systems Security con Kaspersky Security Center".

Se pueden usar variables del entorno al especificar la ruta al origen de actualizaciones en esta tarea. Si se utilizan las variables del entorno de un usuario, ejecute el comando `KAVSHELL UPDATE` con los permisos de dicho usuario.

Sintaxis del comando KAVSHELL UPDATE

```
KAVSHELL UPDATE < Ruta al origen de actualizaciones | /AK | /KL> [/NOUSEKL]
[/PROXY:<dirección>:<puerto>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<nombre de usuario>]
[/PROXYPWD:<contraseña>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE]
[/TIMEOUT:<segundos>] [/REG:<código iso3166>] [/W:<ruta del archivo del registro
de ejecución de la tarea>] [/ALIAS:<alias de la tarea>]
```

El comando KAVSHELL UPDATE tiene claves obligatorias y opcionales (consulte la tabla a continuación).

Ejemplos del comando KAVSHELL UPDATE

- *Para iniciar una tarea de actualización de bases de datos personalizada, ejecute el comando siguiente:*

```
KAVSHELL UPDATE
```

- *Para iniciar una tarea de actualización de bases de datos mediante los archivos de actualizaciones en la carpeta de red \\server\databases, ejecute el siguiente comando:*

```
KAVSHELL UPDATE \\server\databases
```

- *Para iniciar una tarea de actualización usando el servidor FTP ftp://dnl-ru1.kaspersky-labs.com/ y registrar todos los eventos de tareas al archivo de registro c:\update_report.log, ejecute el comando:*

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

- *Para descargar actualizaciones de la base de datos de Kaspersky Embedded Systems Security del servidor de actualización de Kaspersky Lab, conéctese al origen de actualizaciones a través de un servidor proxy (dirección del servidor proxy: proxy.company.com, puerto: 8080). Para acceder al equipo con la autenticación NTLM incorporada de Microsoft Windows con el nombre de usuario: inetuser, contraseña: 123456, y ejecute el siguiente comando:*

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
/PROXYPWD:123456
```

Tabla 88. Claves del comando KAVSHELL UPDATE

Clave	Descripción
Origen de actualizaciones (clave obligatoria). Especifique una o varias fuentes. Kaspersky Embedded Systems Security accederá a los orígenes en el orden en que están enumerados. Delimite las fuentes con un espacio.	

Clave	Descripción
<ruta en formato UNC>	Origen de actualizaciones definido por el usuario. Ruta a la carpeta de actualizaciones de red en formato UNC.
<URL>	Origen de actualizaciones definido por el usuario. Dirección del servidor HTTP o FTP en que se ubica la carpeta de actualización.
<Carpeta local>	Origen de actualizaciones definido por el usuario. Carpeta en el equipo protegido.
/AK	El servidor de administración de Kaspersky Security Center como el origen de actualizaciones.
/KL	Los servidores de actualizaciones de Kaspersky Lab como origen de actualizaciones.
/NOUSEKL	No utilice los servidores de actualizaciones de Kaspersky Lab si no hay otros orígenes de actualizaciones disponibles (se utiliza de manera predeterminada).
Configuración del servidor proxy	
/PROXY:<dirección>:<puerto>	Nombre de red o dirección IP del servidor proxy y su puerto. Si no se especifica esta clave, Kaspersky Embedded Systems Security detectará automáticamente la configuración del servidor proxy utilizado en la red de área local.
/AUTHTYPE:<0-2>	Esta clave especifica el método de autenticación para acceder al servidor proxy. Puede tener los valores siguientes: **0**: autenticación NTLM integrada de Microsoft Windows; Kaspersky Embedded Systems Security se comunicará con el servidor proxy en la cuenta **Sistema local** (**SYSTEM**) **1**: autenticación NTLM integrada de Microsoft Windows; Kaspersky Embedded Systems Security se comunicará con el servidor proxy en la cuenta con el nombre de inicio de sesión y la contraseña especificados por las claves /PROXYUSER y /PROXYPWD **2**: autenticación por el nombre de inicio de sesión y la contraseña especificados por las claves /PROXYUSER y /PROXYPWD (autenticación básica) Si no se requiere autenticación para acceder al servidor proxy, no es necesario especificar una clave.
/PROXYUSER:<nombre de usuario>	Nombre de usuario que se utilizará para acceder al servidor proxy. Si se especifica el valor de la clave /AUTHTYPE:0, se ignorarán las claves /PROXYUSER:<nombre de usuario> y /PROXYPWD:<contraseña>.
/PROXYPWD:<contraseña>	Contraseña de usuario que se utilizará para acceder al servidor proxy. Si se especifica el valor de la clave /AUTHTYPE:0, se ignorarán las claves /PROXYUSER:<nombre de usuario> y /PROXYPWD:<contraseña>. Si se especifica la clave /PROXYUSER y se omite /PROXYPWD, la contraseña se considerará en blanco.
/NOPROXYFORKL	No use la configuración del servidor proxy para establecer conexión con los servidores de actualizaciones de Kaspersky Lab (se utiliza de manera predeterminada)
/USEPROXYFORCUSTOM	Utilice la configuración del servidor proxy para establecer conexión con los orígenes de actualizaciones definidos por el usuario (no se utiliza de manera predeterminada).

Clave	Descripción
/USEPROXYFORLOCAL	Utilice la configuración del servidor proxy para establecer conexión con los orígenes de actualizaciones locales. Si no se especifica, se aplicará el valor **No usar servidor proxy para las direcciones locales**.
Configuración general de los servidores FTP y HTTP	
/NOFTPPASSIVE	Si se especifica esta clave, Kaspersky Embedded Systems Security usará el modo de equipo FTP activo para establecer conexión con el equipo protegido. Si no se especifica esta clave, Kaspersky Embedded Systems Security usará el modo de equipo FTP pasivo, si es posible.
/TIMEOUT:<cantidad de segundos>	Tiempo de espera de conexión del servidor FTP o HTTP. Si no especifica esta clave, Kaspersky Embedded Systems Security usará el valor predeterminado: 10 seg. El valor de la clave debe ser un número entero.
/REG:<código iso3166>	Configuración regional. Esta clave se utiliza cuando se reciben actualizaciones de los servidores de actualizaciones de Kaspersky Lab. Kaspersky Embedded Systems Security optimiza la carga de actualización en el equipo protegido, ya que selecciona el servidor de actualizaciones más cercano. Como el valor de esta clave, especifique el código de letra del país de ubicación para el equipo protegido de acuerdo con ISO 3166-1, por ejemplo, /REG: gr o /REG:RU. Si esta clave se omite o se especifica un código del país inexistente, Kaspersky Embedded Systems Security detectará la ubicación del equipo protegido según la configuración regional del equipo donde la Consola de la aplicación está instalada.
/ALIAS:<alias de la tarea>	Esta clave le permitirá asignar un nombre temporal a la tarea que se utilizará para acceder a la tarea durante su ejecución. Por ejemplo, se pueden ver las estadísticas de la tarea mediante el comando TASK. El alias de tarea debe ser único entre los alias de tarea de todos los componentes funcionales de Kaspersky Embedded Systems Security. Si no se especificó esta clave, se utiliza el nombre temporal update_<pid_de_kavshell>, por ejemplo, update_1234. En la Consola de la aplicación, a la tarea se le asigna el nombre Update-databases (<fecha hora>), por ejemplo, Update-databases 16/08/2007 5:41:02 p. m.

Clave	Descripción
/W:<ruta del archivo de registro de tareas>	Si se especifica esta clave, Kaspersky Embedded Systems Security guardará el archivo de registro de tareas con el nombre definido por el valor de la clave. El archivo de registro contiene las estadísticas de ejecución, la hora de inicio y finalización (detención) de la tarea, e información sobre los eventos producidos en ella. El registro se utiliza para registrar eventos definidos por la configuración de los registros de tareas y el registro de eventos de Kaspersky Embedded Systems Security en el "Visor de eventos". Se puede especificar la ruta relativa o absoluta del archivo de registro. Si se especifica solo el nombre de archivo sin la ruta, el archivo de registro se creará en la carpeta actual. Si se reinicia el comando con la misma configuración de registro, se sobrescribirá el archivo de registro existente. Se puede visualizar el archivo de registro mientras se ejecuta una tarea. El registro se muestra en el nodo **Registros de tareas** de la Consola de la aplicación. Si se produce un error en Kaspersky Embedded Systems Security al crear el archivo de registro, esto no evitará que el comando se ejecute o muestre un mensaje de error.

Códigos de devolución para el comando KAVSHELL UPDATE (en la página 516).

Reversión de actualizaciones de bases de datos de Kaspersky Embedded Systems Security. KAVSHELL ROLLBACK

El comando `KAVSHELL ROLLBACK` se puede utilizar para realizar una tarea del sistema Reversión de las bases de datos de Kaspersky Embedded Systems Security (reversión de las bases de datos de Kaspersky Embedded Systems Security a la versión anteriormente instalada). El comando se realiza sincrónicamente.

Sintaxis del comando:

```
KAVSHELL ROLLBACK
```

Códigos de devolución para el comando KAVSHELL ROLLBACK (en la página 517).

Administración de inspección de registros. KAVSHELL TASK LOG-INSPECTOR

El comando `KAVSHELL TASK LOG-INSPECTOR` puede usarse para supervisar la integridad del entorno en base al análisis del registro de eventos de Windows.

Sintaxis del comando

```
KAVSHELL TASK LOG-INSPECTOR
```

Ejemplos del comando

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Tabla 89. Modificadores del comando KAVSHELL TASK LOG-INSPECTOR

Clave	Descripción
/START	Inicia la tarea especificada en modo asíncrono.
/STOP	Detiene la tarea especificada.
/STATE	Muestra el estado de la tarea actual (por ejemplo, *En ejecución*, *Completada*, *En pausa*, *Detenida*, *Error*, *Iniciando* o *Recuperando*).
/STATISTICS	Recupera las estadísticas de la tarea: información acerca de la cantidad de objetos procesados desde el inicio de la tarea hasta la actualidad.

Códigos de devolución para el comando KAVSHELL TASK LOG-INSPECTOR (consulte la sección “Códigos de devolución para el comando KAVSHELL TASK LOG-INSPECTOR”, en la página 515).

Cómo habilitar, configurar y deshabilitar el registro de rastreo. KAVSHELL TRACE

El comando `KAVSHELL TRACE` se puede utilizar para habilitar y deshabilitar el registro de seguimiento para todos los subsistemas de Kaspersky Embedded Systems Security y para establecer el nivel de detalle del registro.

Kaspersky Embedded Systems Security escribe la información en los archivos de seguimiento y el archivo de volcado de memoria en formato no cifrado.

Sintaxis del comando KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<ruta de la carpeta de archivo del registro de rastreo>
[/S:<tamaño máximo del registro en megabytes>]
[/LVL:debug|info|warning|error|critical] | /OFF>
```

Si se mantiene el registro de rastreo y desea cambiar su configuración, introduzca el comando `KAVSHELL TRACE` con la clave /ON y especifique la configuración del registro de rastreo con los valores de las claves /S y /LVL (consulte la tabla a continuación).

Tabla 90. Claves del comando KAVSHELL TRACE

Clave	Descripción
/ON	Habilita el registro de rastreo.
/F:<carpeta con archivos de registro de rastreo>	Esta clave especifica la ruta completa a la carpeta en la que se guardarán los archivos de registro de rastreo (obligatorio). Si se especifica la ruta de una carpeta inexistente, no se creará ningún archivo de registro. No es posible especificar las rutas a carpetas en las unidades de red de otros equipos. Si el nombre de la carpeta de la que se especifica la ruta de acceso como el valor de la clave contiene un carácter de espacio, escriba la ruta de esta carpeta entre comillas, por ejemplo: /F:"C\Carpeta de rastreo". Se pueden usar variables del entorno del sistema al especificar la ruta a los archivos de registro de rastreo; no se permiten variables del entorno del usuario.

Clave	Descripción
/S: <tamaño máximo de archivo de registro en megabytes>	Esta clave establece el tamaño máximo de un único archivo de registro de rastreo. Tan pronto como el archivo de registro alcanza el nivel máximo, Kaspersky Embedded Systems Security comenzará a registrar información en un archivo nuevo; y el archivo de registro anterior se guardará. Si no se especifica el valor de esta clave, el tamaño máximo de un archivo de registro será 50 MB.
/LVL:debug|info|warning|error|critical	Esta clave define el nivel de detalle de registro desde máximo (**Toda la información de depuración**) en el que todos los eventos se graban en el registro, hasta mínimo (**Eventos críticos**) en el que solo se registran los eventos críticos. Si no se especifica esta clave, los eventos con el nivel de detalle **Toda la información de depuración** se registrarán en el registro de rastreo.
/OFF	Esta clave deshabilita el registro de rastreo.

Ejemplos del comando KAVSHELL TRACE

► *Para habilitar el registro de rastreo mediante el nivel de detalle **Toda la información de depuración** y el tamaño máximo del registro de 200 MB, y para guardar el archivo de registro en la carpeta C:\Trace Folder, ejecute el comando:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

► *Para habilitar el registro de rastreo mediante el nivel de detalle **Eventos importantes** y para guardar el archivo de registro en la carpeta C:\Trace Folder, ejecute el comando:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

► *Para deshabilitar el registro de rastreo, ejecute el comando:*

```
KAVSHELL TRACE /OFF
```

Códigos de devolución para el comando KAVSHELL TRACE (consulte la sección “Códigos de devolución para el comando KAVSHELL TRACE”, en la página 517).

Desfragmentar archivos de registro de Kaspersky Embedded Systems Security. KAVSHELL VACUUM

Con el comando `KAVSHELL VACUUM` puede desfragmentar los archivos de registro de aplicaciones. Permite evitar los errores de aplicación y sistema debido al almacenamiento de un gran número de archivos de registro creados según los eventos de la aplicación.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Se recomienda aplicar el comando `KAVSHELL VACUUM` para optimizar el almacenamiento de archivos de registro en caso de Análisis a pedido frecuentes e inicios de tareas de actualización. Al ejecutar el comando, Kaspersky Embedded Systems Security renueva una estructura lógica para los archivos de registros de aplicación que se

almacenan en un equipo protegido por la ruta especificada.

De forma predeterminada, los archivos de registro de aplicación se almacenan en C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports. Si ha especificado manualmente otra ruta para almacenar registros, el comando `KAVSHELL VACUUM` ejecuta la desfragmentación para archivos en la carpeta que se especifica en la configuración de registros de Kaspersky Embedded Systems Security.

El tamaño grande de desfragmentación de archivos aumenta el periodo de ejecución del comando `KAVSHELL VACUUM`.

Las tareas de Protección en tiempo real y Control del equipo no están disponibles para realizarse durante la ejecución del comando `KAVSHELL VACUUM`. El proceso de desfragmentación en curso restringe el acceso al registro de Kaspersky Embedded Systems Security y rechaza el registro de eventos. Para evitar la disminución del nivel de seguridad, se recomienda planificar la ejecución del comando `KAVSHELL VACUUM` en el tiempo inactivo con antelación.

► *Para desfragmentar archivos de registros de Kaspersky Embedded Systems Security, ejecute el comando siguiente:*

```
KAVSHELL VACUUM
```

La ejecución del comando es posible si se inicia con los derechos de la cuenta del administrador local.

Limpieza de la base de iSwift. KAVSHELL FBRESET

Kaspersky Embedded Systems Security emplea la tecnología iSwift, que permite que la aplicación evite que se vuelvan a analizar los archivos que no se modificaron desde el último análisis (**Usar la tecnología iSwift**).

Kaspersky Embedded Systems Security crea en la carpeta %SYSTEMDRIVE%\System Volume Information los archivos klamfb.dat y klamfb2.dat, que contienen información sobre objetos limpios que ya se han analizado. El archivo klamfb.dat (klamfb2.dat) aumenta con la cantidad de archivos que analiza Kaspersky Embedded Systems Security. El archivo solo contiene información actual sobre la existencia de archivos en el sistema: si un archivo se elimina, Kaspersky Embedded Systems Security purga la información sobre esto de fidbox.dat.

Para limpiar un archivo, utilice el comando `KAVSHELL FBRESET`.

Tenga en cuenta las siguientes especificaciones para ejecutar el comando `KAVSHELL FBRESET`:

- Durante la limpieza del archivo klamfb.dat mediante el comando KAVSHELL FBRESET, Kaspersky Embedded Systems Security no pausa la protección (a diferencia de los casos de la eliminación manual de klamfb.dat).
- Kaspersky Embedded Systems Security puede aumentar la carga de trabajo del equipo después de que los datos se borran en klamfb.dat. En este caso, Kaspersky Embedded Systems Security analiza todos los archivos a los que se accede por primera vez luego de borrar klamfb.dat. Después del análisis, Kaspersky Embedded Systems Security vuelve a agregar a klamfb.dat la información sobre cada objeto analizado. Si se realizan nuevos intentos para acceder al objeto, la tecnología iSwift impedirá un nuevo análisis del archivo siempre que no se haya modificado.

La ejecución del comando `KAVSHELL FBRESET` solo está disponible si la línea de comandos se inicia mediante la cuenta de SYSTEM.

Cómo habilitar y deshabilitar la creación del archivo de volcado. KAVSHELL DUMP

La creación de instantáneas (archivo de volcado) para los procesos de Kaspersky Embedded Systems Security en casos de interrupción anormal se puede habilitar o deshabilitar mediante el comando `KAVSHELL DUMP` (consulte la tabla a continuación). Además, se pueden tomar instantáneas de memoria de procesos en curso de Kaspersky Embedded Systems Security en cualquier momento.

Para que el archivo de volcado se cree correctamente, el comando `KAVSHELL DUMP` se debe ejecutar mediante la cuenta de sistema local (SYSTEM).

Sintaxis del comando KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<carpeta con el archivo de volcado>|/SNAPSHOT /F:< carpeta con el archivo de volcado> / P:<pid> | /OFF>
```

Tabla 91. Claves del comando KAVSHELL DUMP

Clave	Descripción
/ON	Habilita la creación del archivo de volcado de memoria de proceso en casos de interrupción anormal.
/F:<ruta de la carpeta con archivos de volcado>	Esta clave es obligatoria. Especifica la ruta a la carpeta en la cual se guardará el archivo de volcado. No es posible especificar las rutas a carpetas en las unidades de red de otros equipos no protegidos. Se pueden usar variables del entorno del sistema al especificar la ruta a la carpeta con el archivo de volcado de memoria; no se permiten variables del entorno del usuario.
/SNAPSHOT	Toma una instantánea de la memoria del proceso en curso con un PID especificado y guarda el archivo de volcado en la carpeta de la ruta que está especificada por la clave /F.
/P	El identificador de proceso PID se muestra en el Administrador de tareas de Microsoft Windows.
/OFF	Deshabilita la creación del archivo de volcado de memoria de procesos en casos de interrupción anormal.

Códigos de devolución para el comando KAVSHELL DUMP (consulte la sección “Códigos de devolución para el comando KAVSHELL DUMP”, en la página 518).

Ejemplos del comando KAVSHELL DUMP

► *Para habilitar la creación de un archivo de volcado; para guardar el archivo de volcado en la carpeta C:\Dump Folder, ejecute el comando:*

```
KAVSHELL DUMP /ON /F:”C:\Dump Folder”
```

► *Para realizar un volcado para el proceso con el Id. 1234 a la carpeta C:/Dumps, ejecute el comando:*

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /F:1234
```

► *Para deshabilitar la generación del archivo de volcado, ejecute el comando:*

```
KAVSHELL DUMP /OFF
```

Importación de la configuración. KAVSHELL IMPORT

El comando `KAVSHELL IMPORT` permite importar la configuración de Kaspersky Embedded Systems Security, sus funciones y tareas de un archivo de configuración a una copia de Kaspersky Embedded Systems Security en el equipo protegido. Se puede crear un archivo de configuración mediante el comando `KAVSHELL EXPORT`.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL IMPORT

```
KAVSHELL IMPORT <nombre del archivo de configuración y ruta del archivo>
```

Ejemplos del comando KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Tabla 92. Claves del comando KAVSHELL IMPORT

Clave	Descripción
<nombre del archivo de configuración y ruta del archivo>	Nombre del archivo de configuración utilizado como el origen de importación de la configuración. Se pueden usar variables del entorno del sistema al especificar la ruta al archivo; no se permiten variables del entorno del usuario.

Códigos de devolución para el comando KAVSHELL IMPORT (consulte la sección “Códigos de devolución para el comando KAVSHELL IMPORT”, en la página 519).

Exportación de la configuración. KAVSHELL EXPORT

El comando `KAVSHELL EXPORT` permite exportar todos los valores de configuración de Kaspersky Embedded Systems Security y sus tareas actuales a un archivo de configuración, a fin de importarlos más tarde a copias de Kaspersky Embedded Systems Security instaladas en otro equipo.

Sintaxis del comando KAVSHELL EXPORT

```
KAVSHELL EXPORT <nombre del archivo de configuración y ruta del archivo>
```

Ejemplos del comando KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Tabla 93. Claves del comando KAVSHELL EXPORT

Clave	Descripción
<nombre del archivo de configuración y ruta del archivo>	Nombre del archivo de configuración que contendrá la configuración. Se puede asignar cualquier extensión al archivo de configuración. Se pueden usar variables del entorno del sistema al especificar la ruta al archivo; no se permiten variables del entorno del usuario.

Códigos de devolución para el comando KAVSHELL EXPORT (consulte la sección “Códigos de devolución para el comando KAVSHELL EXPORT”, en la página 519).

Integración con Microsoft Operations Management Suite. KAVSHELL OMSINFO

Con el comando KAVSHELL OMSINFO, puede revisar el estado de la aplicación, además de información sobre amenazas detectadas por bases de datos antivirus y el servicio KSN. Los datos sobre amenazas se toman desde los registros de eventos disponibles.

Sintaxis del comando KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <ruta de acceso completa al archivo generado con nombre de archivo>
```

Ejemplos del comando KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Tabla 94. Claves del comando KAVSHELL OMSINFO

Clave	Descripción
<ruta de acceso al archivo generado con nombre de archivo>	El nombre del archivo generado, que contendrá información sobre el estado de aplicación y las amenazas detectadas.

Códigos de devolución de la línea de comandos

En esta sección

Código de devolución para los comandos KAVSHELL START y KAVSHELL STOP

Tabla 95. Código de devolución para los comandos KAVSHELL START y KAVSHELL STOP

Código de devolución	Descripción
0	Operación finalizada correctamente
-3	Error de permisos
-5	Sintaxis de comando no válida
-6	Operación no válida (por ejemplo, el servicio de Kaspersky Embedded Systems Security ya está en ejecución o detenido)
-7	Servicio no registrado
-8	El inicio de Servicio automático está deshabilitado.
-9	Error en el intento de inicio del equipo desde otra cuenta de usuario (de manera predeterminada, el servicio de Kaspersky Embedded Systems Security se ejecuta desde la cuenta de usuario Sistema local)
-99	Error desconocido

Código de devolución para los comandos KAVSHELL SCAN y KAVSHELL SCANCRITICAL

Tabla 96. Código de devolución para los comandos KAVSHELL SCAN y KAVSHELL SCANCRITICAL

Código de devolución	Descripción
0	La operación se completó correctamente (no se detectaron amenazas)
1	Operación cancelada
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (no se encontró el archivo con la lista de áreas de análisis)
-5	Sintaxis de comando no válida o área del análisis sin definir
-80	Objetos infectados y otros objetos detectados
-81	Objetos probablemente infectados detectados
-82	Errores de proceso detectados
-83	Objetos sin comprobar detectados
-84	Objetos dañados detectados
-85	Error de creación de archivo de registro de tareas

Código de devolución	Descripción
-99	Error desconocido
-301	Clave no válida

Códigos de devolución para el comando KAVSHELL TASK LOG-INSPECTOR

Tabla 97. Código de devolución para el comando KAVSHELL TASK LOG-INSPECTOR

Código de devolución	Descripción
0	Operación finalizada correctamente
-6	Operación no válida (por ejemplo, el servicio de Kaspersky Embedded Systems Security ya está en ejecución o detenido)
402	La tarea ya se está ejecutando (para el modificador /STATE)

Códigos de devolución para el comando KAVSHELL TASK

Tabla 98. Códigos de devolución para el comando KAVSHELL TASK

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (tarea no encontrada)
-5	Sintaxis de comando no válida
-6	Operación no válida (por ejemplo, la tarea no se está ejecutando, ya se está ejecutando o no se puede pausar)
-99	Error desconocido
-301	Clave no válida
401	La tarea no se está ejecutando (para el modificador /STATE)
402	La tarea ya se está ejecutando (para el modificador /STATE)
403	La tarea ya está en pausa (para el modificador /STATE)
-404	Error al ejecutar la operación (el cambio de estado de tarea provocó una interrupción del funcionamiento)

Códigos de devolución para el comando KAVSHELL RTP

Tabla 99. Códigos de devolución para el comando KAVSHELL RTP

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (una de las tareas de Protección en tiempo real o todas las tareas de Protección en tiempo real no han sido encontradas)
-5	Sintaxis de comando no válida
-6	Operación no válida (por ejemplo, la tarea ya está en ejecución o detenida)
-99	Error desconocido
-301	Clave no válida

Códigos de devolución para el comando KAVSHELL UPDATE

Tabla 100. Códigos de devolución para el comando KAVSHELL UPDATE

Código de devolución	Descripción
0	Operación finalizada correctamente
200	Todos los objetos están actualizados (base de datos o componentes del programa actuales)
-2	El servicio no está en ejecución
-3	Error de permisos
-5	Sintaxis de comando no válida
-99	Error desconocido
-206	Faltan archivos de extensión en la fuente especificada o estos tienen un formato desconocido
-209	Error al conectarse al origen de actualizaciones
-232	Error de autenticación al conectarse al servidor proxy
-234	Error al conectarse a Kaspersky Security Center
-235	Kaspersky Embedded Systems Security no fue autenticado al conectarse al origen de actualizaciones
-236	La base de datos de la aplicación está dañada
-301	Clave no válida

Códigos de devolución para el comando KAVSHELL ROLLBACK

Tabla 101. Códigos de devolución para el comando KAVSHELL ROLLBACK

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-99	Error desconocido
-221	Copia de seguridad de la base de datos no encontrada o dañada
-222	Copia de seguridad de la base de datos dañada

Códigos de devolución para el comando KAVSHELL LICENSE

Tabla 102. Códigos de devolución para el comando KAVSHELL LICENSE

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Privilegios insuficientes para administrar claves
-4	No se encontró la clave con el número especificado
-5	Sintaxis de comando no válida
-6	Operación no válida (clave ya agregada)
-99	Error desconocido
-301	Clave no válida
-303	La licencia se aplica a una aplicación diferente

Códigos de devolución para el comando KAVSHELL TRACE

Tabla 103. Códigos de devolución para el comando KAVSHELL TRACE

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución

Código de devolución	Descripción
-3	Error de permisos
-4	No se encontró el objeto (no se encontró la ruta especificada de la carpeta Registros de rastreo)
-5	Sintaxis de comando no válida
-6	Operación no válida (intento de ejecución del comando KAVSHELL TRACE /OFF si la creación de registros de rastreo ya está deshabilitada)
-99	Error desconocido

Códigos de devolución para el comando KAVSHELL FBRESET

Tabla 104. Códigos de devolución para el comando KAVSHELL FBRESET

Código de devolución	Descripción
0	Operación finalizada correctamente
-99	Error desconocido

Códigos de devolución para el comando KAVSHELL DUMP

Tabla 105. Códigos de devolución para el comando KAVSHELL DUMP

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (no se encontró la ruta especificada de la carpeta del archivo de volcado; no se encontró el proceso con el PID especificado)
-5	Sintaxis de comando no válida
-6	Operación no válida (intento de ejecución del comando KAVSHELL DUMP/OFF si la creación de archivos de volcado ya está deshabilitada)
-99	Error desconocido

Códigos de devolución para el comando KAVSHELL IMPORT

Tabla 106. Códigos de devolución para el comando KAVSHELL IMPORT

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (no se encontró el archivo de configuración para importación)
-5	Sintaxis no válida
-99	Error desconocido
501	La operación finalizó correctamente. Sin embargo, se produjo un error/comentario durante la ejecución del comando, por ejemplo, Kaspersky Embedded Systems Security no importó los parámetros de algunos componentes funcionales
-502	Falta el archivo que se está importando o el formato no se reconoce
-503	Configuración incompatible (archivo de configuración exportado desde un programa diferente o desde una versión posterior e incompatible de Kaspersky Embedded Systems Security)

Códigos de devolución para el comando KAVSHELL EXPORT

Tabla 107. Códigos de devolución para el comando KAVSHELL EXPORT

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-5	Sintaxis no válida
-10	No es posible crear el archivo de configuración (por ejemplo, no hay acceso a la carpeta especificada en la ruta del archivo)
-99	Error desconocido
501	La operación finalizó correctamente. Sin embargo, se produjo un error/comentario durante la ejecución del comando, por ejemplo, Kaspersky Embedded Systems Security no exportó los parámetros de algunos componentes funcionales

Comunicarse con el soporte técnico

Esta sección describe cómo se puede recibir soporte técnico y las condiciones en las cuales se encuentra disponible.

En este capítulo

Cómo acceder al Servicio de soporte técnico

Si no encuentra una solución a su problema en la documentación de la aplicación ni en ninguna de las fuentes de información sobre la aplicación, le recomendamos que se comunique con el Servicio de soporte técnico. Los especialistas del soporte técnico responderán sus preguntas acerca de la instalación y el uso de la aplicación.

El soporte técnico se encuentra disponible solo para los usuarios que adquirieron una licencia comercial de la aplicación. El soporte técnico no está disponible para los usuarios que tienen una licencia de prueba.

Antes de ponerse en contacto con el servicio de soporte técnico, lea rápidamente las reglas del Servicio de soporte técnico.

Puede comunicarse con el soporte técnico en una de las siguientes maneras:

- Llamando al servicio de soporte técnico.
- Enviando una solicitud al servicio de soporte técnico de Kaspersky Lab por medio del portal de Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Obtener servicio de soporte técnico por teléfono

Puede llamar a los especialistas de servicio de soporte técnico desde casi todas las regiones del mundo. Puede encontrar información sobre cómo obtener servicio de soporte técnico en su región e información de contacto del Soporte Técnico en el sitio web del Soporte técnico de Kaspersky Lab (https://support.kaspersky.com/b2b/).

Antes de ponerse en contacto con el servicio de soporte técnico, lea rápidamente las reglas de soporte (https://support.kaspersky.com/support/rules/es_mx).

Soporte técnico mediante Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) es un portal para empresas que usan aplicaciones de Kaspersky Lab. Kaspersky CompanyAccount está diseñado para facilitar la interacción entre usuarios y especialistas de Kaspersky Lab mediante solicitudes en línea. El portal de Kaspersky CompanyAccount le permite supervisar el progreso del procesamiento de solicitud electrónico por parte de especialistas de Kaspersky Lab y almacenar un historial de solicitudes electrónicas.

Puede registrar a todos los empleados de su organización en una única cuenta de usuario en Kaspersky CompanyAccount. Una única cuenta le permite administrar de manera centralizada las solicitudes electrónicas de empleados registrados en Kaspersky Lab y también gestionar los privilegios de dichos empleados mediante Kaspersky CompanyAccount.

Kaspersky CompanyAccount se encuentra disponible en los siguientes idiomas:

- Inglés
- Español
- Italiano
- Alemán
- Polaco
- Portugués
- Ruso
- Francés
- Japonés

Para obtener más información sobre Kaspersky CompanyAccount, visite el sitio web del servicio de soporte técnico https://support.kaspersky.com/mx/faq/companyaccount_help.

Uso de archivos de rastreo y scripts AVZ

Después de informar un problema a los especialistas del Servicio de soporte técnico de Kaspersky Lab, es posible que le soliciten que genere un informe con datos sobre el funcionamiento de Kaspersky Embedded Systems Security y que lo envíe al Servicio de soporte técnico de Kaspersky Lab. También es posible que los especialistas del servicio de soporte técnico de Kaspersky Lab le pidan que cree un archivo de rastreo. El archivo de rastreo le permite seguir el proceso de cómo se llevan a cabo los comandos de la aplicación, paso a paso, a fin de determinar la etapa de funcionamiento de la aplicación en la que se produce el error.

Luego de analizar los datos que envíe, los especialistas de soporte técnico de Kaspersky Lab pueden crear un script AVZ y enviárselo. Mediante los scripts AVZ resulta posible analizar procesos activos en busca de amenazas, analizar el equipo en busca de amenazas, desinfectar o eliminar archivos infectados y crear informes de análisis del sistema.

Para una mayor eficacia en la asistencia y la solución de problemas de la aplicación, es posible que los especialistas del Servicio de soporte técnico le soliciten que cambie la configuración de la aplicación temporalmente con fines de depuración durante el diagnóstico. Esto puede requerir que realice lo siguiente:

- Activar la funcionalidad que procesa y almacena información diagnóstica ampliada.
- Afinar la configuración de los componentes individuales de la aplicación, que no están disponibles

mediante los elementos de la interfaz de usuario estándar.

- Cambiar la configuración del almacenamiento y la transmisión de la información de diagnóstico que se procesa.
- Configurar la interceptación y el registro del tráfico de red.

Glosario

A

Actualización

El procedimiento de sustituir o agregar archivos nuevos (bases de datos o módulos de la aplicación) que se recuperaron de los servidores de actualizaciones de Kaspersky Lab.

Analizador heurístico

Una tecnología para detectar amenazas sobre la información que aún no se ha agregado a las bases de datos de Kaspersky Lab. El analizador heurístico detecta objetos que, por su comportamiento, pueden ser una amenaza para la seguridad del sistema operativo. Los objetos detectados por el analizador heurístico se consideran probablemente infectados. Por ejemplo, un objeto se puede considerar posiblemente infectado si contiene secuencias de comandos que son habituales de objetos maliciosos (abrir archivo, escribir en el archivo).

Archivo comprimido

Uno o varios archivos empaquetados en un solo archivo a través de la compresión. Se requiere una aplicación dedicada, denominada archivador, para comprimir y descomprimir los datos.

Archivo infectable

Un archivo que, debido a su estructura o formato, puede ser utilizado por criminales como “contenedor para almacenar y extender código malicioso. Como regla general, se trata de archivos ejecutables con extensiones de archivo como .com, .exe, y .dll. El riesgo de penetración del código malicioso en estos archivos es bastante alto.

B

Bases de datos antivirus

Bases de datos que contienen información sobre amenazas a la seguridad de los equipos que son conocidas por Kaspersky Lab a la fecha de publicación de las bases de datos antivirus. Las entradas en las bases de datos antivirus permiten que se detecte código malicioso en objetos analizados. Las bases de datos antivirus son creadas por especialistas de Kaspersky Lab y se actualizan cada hora.

C

Clave activa

Una clave que es utilizada actualmente por la aplicación.

Configuración de tareas

Configuración de la aplicación que es específica de cada tipo de tarea.

Copia de seguridad

Un almacenamiento especial para copias de seguridad de archivos, que se crean antes de intentar operaciones de desinfección o eliminación.

Cuarentena

Carpeta a la que la aplicación Kaspersky Lab pasa los objetos probablemente infectados que se han detectado.

Los objetos se almacenan en Cuarentena de forma cifrada con el fin de evitar cualquier efecto en el equipo.

D

Desinfección

Método de procesamiento de objetos infectados que produce una recuperación total o parcial de datos. No todos los objetos infectados se pueden desinfectar.

Directiva

Una directiva determina la configuración de una aplicación y maneja la capacidad de configurar esa aplicación en equipos dentro de un grupo de administración. Debe crearse una directiva particular para cada aplicación. Puede crear un número ilimitado de diferentes directivas para aplicaciones instaladas en equipos en cada grupo de administración, pero solo se puede aplicar una directiva por vez a cada aplicación de forma simultánea dentro de un grupo de administración.

E

Estado de protección

El estado de protección actual, que refleja el nivel de seguridad del equipo.

F

Falso positivo

Una situación en la cual una aplicación de Kaspersky Lab considera que un objeto no infectado está infectado porque su código es similar al de un virus.

G

Gravedad del evento

Propiedad de un evento encontrada durante la operación de una aplicación de Kaspersky Lab. Hay cuatro niveles de gravedad:

- Evento crítico.
- Error.
- Advertencia.
- Información.

Los eventos del mismo tipo pueden tener niveles de gravedad diferentes según la situación en la cual se produjeron.

K

Kaspersky Security Network (KSN)

Una infraestructura de servicios en la nube que permite acceder a la base de datos de Kaspersky Lab con información constantemente actualizada sobre la reputación de archivos, recursos web y software. Kaspersky Security Network asegura respuestas más rápidas por parte de aplicaciones de Kaspersky Lab a amenazas,

mejora el rendimiento de algunos componentes de protección y reduce la posibilidad de falsos positivos.

M

Máscara de archivo

Representación de un nombre de archivo con comodines. Los comodines estándar utilizados en máscaras del archivo son * y ?, dónde * representa cualquier número de cualquier cantidad de caracteres, y ? representa cualquier carácter.

N

Nivel de seguridad

El nivel de seguridad se define como un conjunto preconfigurado de opciones del componente de la aplicación.

O

Objeto infectado

Un objeto que posee una porción de código coincide completamente con parte de código de malware conocido. Kaspersky Lab no recomienda acceder a esos objetos.

Objeto OLE

Un objeto vinculado a otro archivo o integrado en otro archivo a través del uso de la tecnología Object Linking and Embedding (OLE). Un ejemplo de un objeto OLE es una hoja de cálculo de Microsoft Office Excel® integrada en un documento de Microsoft Office Word.

Objetos de inicio

Un conjunto de aplicaciones necesario para que el sistema operativo y el software que está instalado en el equipo se inicie y funcione correctamente. Estos objetos se ejecutan cada vez que se inicia el sistema operativo. Hay virus capaces de infectar específicamente estos objetos y que pueden conducir, por ejemplo, al bloqueo del inicio del sistema operativo.

P

Protección en tiempo real

Modo de funcionamiento de la aplicación en el cual se analizan los objetos para detectar la presencia de código malicioso en tiempo real.

La aplicación intercepta todos los intentos de abrir un objeto (leer, escribir o ejecutar) y analiza el objeto para detectar amenazas. Los objetos no infectados se pasan al usuario, mientras que los objetos que contienen amenazas u objetos probablemente infectados se procesan según la configuración de la tarea (desinfectado, eliminado o en cuarentena).

S

Servidor de administración

Un componente de Kaspersky Security Center que almacena centralmente la información sobre todas las aplicaciones de Kaspersky Lab que se instalan dentro de la red corporativa. También puede usarse para

administrar estas aplicaciones.

SIEM

Una tecnología que analiza eventos de seguridad que provienen de varias aplicaciones y dispositivos de red.

T

Tarea

Las funciones realizadas por la aplicación Kaspersky Lab se implementan como tareas, por ejemplo: Protección de archivos en tiempo real, Análisis completo y Actualización de bases de datos.

Tarea local

Una tarea definida y en ejecución en un solo equipo cliente.

Término de la licencia

Un periodo de tiempo durante el cual se tiene acceso a las funciones de la aplicación y a derechos de usar servicios adicionales. Los servicios que se pueden usar dependen del tipo de la licencia.

V

Vulnerabilidad

Una falla en un sistema operativo o una aplicación que puede ser utilizada por programadores de malware para penetrar en el sistema operativo o la aplicación y corromper su integridad. Presencia de una gran cantidad de vulnerabilidades en el sistema operativo que no lo hacen de confianza, debido a que los virus que penetraron en el sistema operativo pueden ocasionar alteraciones en él y en las aplicaciones instaladas.

AO Kaspersky Lab

Kaspersky Lab es un proveedor de fama internacional de sistemas para proteger equipos contra diferentes tipos de amenazas digitales, incluidos virus y otro malware, correo electrónico no solicitado (spam), ataques de hackers y de redes.

En 2008, Kaspersky Lab fue clasificado entre los cuatro mayores proveedores del mundo en cuanto a soluciones de software de seguridad de información para usuarios finales (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab es el proveedor preferido de sistemas de protección de equipos domésticos en Rusia (IDC Endpoint Tracker 2014).

Kaspersky Lab se creó en Rusia en 1997. Desde entonces, se ha convertido en un grupo internacional de compañías con 38 oficinas en 33 países. La compañía emplea a más de 3000 profesionales especializados.

Productos. Los productos de Kaspersky Lab proporcionan protección para todos los sistemas, desde equipos domésticos hasta grandes redes corporativas.

La gama de productos personales incluye aplicaciones de seguridad para equipos de escritorio, equipos portátiles, equipos tablet, teléfonos inteligentes y otros dispositivos móviles.

La empresa ofrece soluciones de protección y control, y tecnologías para estaciones de trabajo y dispositivos móviles, máquinas virtuales, servidores de archivos y web, puertas de enlace de correo y firewalls. La cartera de productos de la compañía incluye además productos especializados que ofrecen protección contra ataques de DDoS, protección para sistemas de control industriales y prevención de fraude financiero. Utilizado en conjunto con herramientas de administración centralizadas, estas soluciones garantizan una protección automatizada efectiva para compañías y organizaciones contra amenazas de equipos de cualquier tamaño. Los productos de Kaspersky Lab están certificados por importantes laboratorios de pruebas, son compatibles con software de diferentes proveedores y están optimizados para funcionar en varias plataformas de hardware.

Los analistas de virus de Kaspersky Lab trabajan las 24 horas. Todos los días, descubren cientos de miles de amenazas informáticas nuevas, crean herramientas para detectarlas y desinfectarlas, e incluyen sus firmas en las bases de datos que utilizan las aplicaciones de Kaspersky Lab.

Tecnologías. Muchas tecnologías que ahora son parte integral de las herramientas antivirus modernas fueron desarrolladas por Kaspersky Lab. No es ninguna coincidencia que muchos otros desarrolladores usen el motor de Kaspersky Anti-Virus en sus productos, entre ellos: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu y ZyXEL. Muchas de las tecnologías innovadoras de la compañía están patentadas.

Logros. Con el paso de los años, Kaspersky Lab ha obtenido cientos de premios por sus servicios para combatir las amenazas informáticas. Después de las pruebas y la investigación realizadas por el prestigioso laboratorio de pruebas austríaco AV-Comparatives en 2014, Kaspersky Lab se clasificó entre los dos primeros proveedores por el número de certificados Advanced+ que obtuvo y, finalmente, se le otorgó el certificado de clasificación más alta. Sin embargo, el logro principal de Kaspersky Lab es la lealtad de sus usuarios en todo el mundo. Los productos y las tecnologías de la compañía protegen a más de 400 millones de usuarios, y sus clientes corporativos suman más de 270 000.

Sitio web de Kaspersky Lab:	https://latam.kaspersky.com/
Enciclopedia de Virus:	https://securelist.lat/
Kaspersky VirusDesk:	https://virusdesk.kaspersky.com/ (para analizar archivos y sitios web sospechosos)
Comunidad web de Kaspersky Lab:	https://community.kaspersky.com

Información sobre código de terceros

La información sobre código de terceros se encuentra en el archivo denominado legal_notices.txt, en la carpeta de instalación de la aplicación.

Avisos de marcas registradas

Las marcas comerciales registradas y las marcas de servicio son propiedad de sus respectivos titulares.

Intel y Pentium son marcas comerciales de Intel Corporation en los Estados Unidos y/u otros países.

Linux es la marca comercial registrada de Linus Torvalds en los Estados Unidos y otros países.

Microsoft, Active Directory, Excel, Internet Explorer, y Windows son marcas comerciales registradas de Microsoft Corporation en los Estados Unidos y otros países.

UNIX es una marca comercial registrada en los Estados Unidos y otros países, licenciada exclusivamente a través de X/Open Company Limited.

Índice

A

C

D

E

I

M

O

P

R

S

T

V